Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ПОРЕМСЬКИЙ МИХАЙЛО ВАСИЛЬОВИЧ

УДК 621.391:519.2:510.5

ДИСЕРТАЦІЯ
МЕТОДИ ОБҐРУНТУВАННЯ СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК НАД СКІНЧЕННИМИ ПОЛЯМИ ПОРЯДКУ 2^r

125 – «Кібербезпека»
12 – «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ М.В. Поремський

Науковий керівник
Олексійчук Антон Миколайович, доктор технічних наук, доцент

Київ – 2020

АНОТАЦІЯ

Поремський М.В. Методи обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над скінченними полями характеристики 2^r – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека. – Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2020.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі, яка полягає у розробці методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак.

Забезпечення інформаційної безпеки держави є однією із найважливіших задач в умовах великої кількості внутрішніх та зовнішніх загроз, які безпосередньо впливають на її економічну стабільність та суверенітет. Таким чином, першочерговими задачами у сфері інформаційної безпеки держави є розробка нових та вдосконалення існуючих криптографічних систем. Кожна така система повинна задовольняти певним вимогам, а саме забезпечувати необхідний рівень швидкості роботи (як в сучасних бездротових мережах), забезпечувати достатній рівень стійкості та ефективно працювати на сучасних комп'ютерних процесорах. Усім цим вимогам задовольняють потокові шифри (ПШ), які широко використовуються в сучасних захищених мережевих протоколах, стандартах мобільного зв'язку, системах супутникового зв'язку та в апаратних застосуваннях з обмеженими ресурсами. Потокові шифри широко вивчаються світовою спільнотою, про що говорить низка міжнародних конкурсів, а також конкурсів в окремих державах.

З розвитком інформаційних технологій та комп'ютерної техніки значну увагу привернули до себе слово-орієнтовані ПШ, які є програмно-орієнтованими та можуть ефективно працювати на сучасних процесорах. Порівняльні дослідження алгоритмів потокового шифрування показують, що одним із найкращих серед сучасних ПШ є шифр SNOW 2.0, що є на сьогодні міжнародним стандартом. В свою чергу, взявши шифр SNOW 2.0 як прототип, було створено важливий клас SNOW 2.0-подібних ПШ. До цього класу відноситься і нещодавно створений в Україні шифр "Струмок", прийнятий як національний стандарт ДСТУ 8845:2019. Важливою частиною процесу розробки таких шифрів, що зумовлює вибір окремих компонент і параметрів для їх побудови, є обґрунтування їх стійкості відносно усіх відомих на сьогодні атак.

Сучасні методи криптоаналізу потокових шифрів, а також атаки, що будуються на їх основі, звичайно поділяють на методи "зламування", спрямовані на відновлення ключів (або початкових станів генераторів гами), та методи, призначені для виявлення певних відмінностей між вихідними послідовностями генератора і випадковими послідовностями. При цьому, в залежності від інформації, що доступна криптоаналітику класи атак можна поділити на атаки на основі відомого шифрованого тексту, атаки на основі відомого відкритого тексту та атаки на основі відомих або підібраних векторів ініціалізації. Крім перелічених видів атак, які проводяться за умови застосування єдиного невідомого ключа шифрування, розглядають також атаки зі зв'язаними ключами, при проведенні яких противник, маючи доступ до декількох шифрувальних перетворень, намагається відновити відповідні їм ключі, використовуючи певні відомі співвідношення між ними. На сьогодні відомо декілька видів атак, запропонованих на SNOW 2.0, які, в принципі, можуть бути застосовані до будь-якого SNOW 2.0-подібного потокового

шифру. Це атаки зі зв'язаними ключами, узагальнена статистична атака та низка пов'язаних з нею атак, алгебраїчна атака та широкий клас кореляційних атак.

Аналіз доступних публікацій показує, що найбільш потужними атаками на SNOW 2.0 (складність яких може бути помітно менше складності повного перебору ключів) є кореляційні атаки, які базуються на побудові та розв'язанні систем лінійних рівнянь зі спотвореними правими частина над полями порядку 2^r, де $r \geq 2$. При цьому виявляється, що методи, розвинуті для оцінювання стійкості до таких атак саме шифру SNOW 2.0, стають незастосовними у випадку SNOW-2.0-подібних шифрів, які будуються над полями порядку 2^{64} або більше (наприклад, для шифру "Струмок"). В цілому, на сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість SNOW-2.0-подібних ПШ відносно відомих кореляційних атак безпосередньо за параметрами їх компонент.

В роботі удосконалено аналітичну оцінку інформаційної складності кореляційних атак на потокові шифри. На відміну від раніше відомої (евристичної) оцінки, отримана аналітична оцінка має належне наукове обґрунтування, містить явну залежність від ймовірності помилки атаки та є справедливою для будь-яких кореляційних атак на потокові шифри незалежно від способу побудови або методу розв'язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

Вперше отримано аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри. На відміну від відомих співвідношень, які визначають квадратичну евклідову незбалансованість, отримане співвідношення встановлює вираз цього параметра в термінах коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Це дозволяє отримувати нижні оцінки трудомісткості й

обсягу матеріалу, потрібного для реалізації кореляційних атак на SNOW 2.0-подібні шифри та порівнювати за трудомісткістю та обсягом матеріалу кореляційні атаки, що будуються над полями різних порядків.

Вперше розроблено метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на полем з двох елементів, розроблений метод базується на отриманому дисертантом аналітичному співвідношенні для параметра, який характеризує ефективність атаки, та дозволяє обґрунтовувати стійкість двійкових SNOW 2.0-подібних потокових шифрів безпосередньо за параметрами їх компонент.

Отримав подальший розвиток метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на SNOW 2.0, розроблений метод базується на отриманих дисертантом аналітичних співвідношеннях, які узагальнюють низку окремих результатів про матричні представлення незбалансованості відображень, що реалізуються скінченними автоматами. Розроблений метод є застосовним до модулярних r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування.

Практичне значення одержаних результатів полягає в тому, що дисертантом розроблено програмні реалізації, які дозволяють в режимі реального часу обчислювати значення нижніх меж трудомісткості та обсягу матеріалу, потрібного для здійснення будь-якої з відомих кореляційних атак на довільний двійковий чи модулярний SNOW 2.0-подібний шифр з вузлами заміни довжини 8 бітів. Розроблені програми застосовані для обґрунтування стійкості шифру “Струмок”, а також його двійкової версії. Вони можуть бути

використані на практиці при дослідженні стійкості інших SNOW 2.0-подібних потокових шифрів у СІТС України.

Наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України – в результаті виконання НДР “Корифена” та в науково-технічних розробках ЗАО “Інститут інформаційних технологій”.

Ключові слова: кібербезпека, потоковий шифр, кореляційна атака, криптоаналіз, обґрунтування стійкості.

ABSTRACT

Poremskyi M. Methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks over finite fields of order 2^r. – Qualifying scientific work as a manuscript.

Ph.D thesis in the field of knowledge 12 Information technologies in specialty 125 Cybersecurity. – Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, 2018.

This thesis is devoted to solving actual scientific problem of development the methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks.

Ensuring the information security of the country is one of the most important tasks in the context of a large number of internal and external threats that affect its economic stability and sovereignty. Thus, the priority in the field of information security of the country is the creation of new and improvement of existing cryptographic systems. Each such system must meet certain requirements, namely to provide the necessary level of speed (as in modern wireless networks), to provide a sufficient level of security and to work efficiently on modern computer processors. All of these requirements are met by stream ciphers (SC), which are widely used in

modern secure network protocols, mobile communications standards, satellite communications and hardware applications with limited resources. Streaming ciphers are widely studied by the international community, as evidenced by a number of international competitions as well as competitions in separate countries.

With the advancement of information and computer technologies, significant attention has been drawn to word-based SC that are software-oriented and can run efficiently on modern processors. Comparative studies of stream encryption algorithms show that one of the best among current SC is SNOW 2.0, which is currently the international standard. In turn, using SNOW 2.0 cipher as a prototype, an important class of SNOW 2.0-like ciphers was created. This class includes the recently created in Ukraine cipher "STRUMOK", adopted as the national standard DSTU 8845: 2019. An important part of the process of developing such ciphers, which determines the choice of individual components and parameters for their construction, is their security evaluatin against all known attacks.

Current methods of cryptanalysis of stream ciphers, as well as the attacks based on them, are usually divided into "hacking" methods aimed at recovering keys (or initial states of gamma generators), and methods designed to detect certain differences between the original sequences of the generator and random sequences. However, depending on the information available to the crypto analyst, the classes of attacks can be divided into attacks based on known encrypted text, attacks based on known plaintext, and attacks based on known or selected initialization vectors. In addition to the types of attacks that are conducted using a single unknown encryption key, attacks with related keys, during which the adversary, having access to several encryption transformations, attempts to recover their respective keys using certain known ratios between them are also considered. Today, there are several types of attacks proposed on SNOW 2.0 that, in principle, can be applied to any SNOW 2.0-like stream cipher. These are related-key attacks, a generalized statistical attack and a set of related attacks, algebraic attack and a wide range of correlation attacks.

Analysis of available scientific publications was carried out. It shows that the most powerful attacks on SNOW 2.0 (the complexity of which can be much less than complexity of a complete key search) are correlation attacks, which are based on creating and solving systems of linear equations with right sides corrupted by noise over the fields of order 2^r, where $r \geq 2$. It turns out that the methods developed for security evaluation against such attacks, namely SNOW 2.0, become inapplicable in the case of SNOW-2.0-like ciphers that are built over fields of order 2^{64} or more (for example, for cipher "Strumok"). In general, there are currently no methods that can evaluate a security of SNOW-2.0-like ciphers against known correlative attacks directly by the parameters of their components.

The analytical estimation of information complexity of correlation attacks on stream ciphers is improved in thesis. Unlike the previously known (heuristic) estimate, the analytical estimate obtained has a scientific basis, contains a clear dependence on the probability of an error of attack and is valid for any correlation attacks on stream ciphers, regardless of the method of creation or solving the system of equations with right parts corrupted by noise, which is creating on the first stage of the attack.

For the first time, an analytical relation was obtained for the quadratic Euclidean imbalance of the probability distribution of corruptions in the right part of the equations that are used to construct correlation attacks on SNOW 2.0-like ciphers. Unlike the known correlations that determine the quadratic Euclidean imbalance, the obtained relation determines the expression of this parameter in terms of the Fourier coefficients of the corruption in the right part of the equations of a single system that does not dependent on particular attack. This allows us to obtain lower bounds of the complexity and amount of material required to SNOW 2.0-like correlation attack on SNOW 2.0-like ciphers and to compare the complexity and amount of material for different correlation attacks that are built over fields of different orders.

For the first time a method of security evaluation of binary SNOW 2.0-like ciphers against correlation attacks over finite fields of characteristic 2 was developed. In contrast to the known approaches of creating correlation attacks over a field of two elements, the developed method is based on the analytic correlation obtained by researcher for the parameter that characterize the attack efficiency and allows to evaluate the security of binary SNOW 2.0-like stream ciphers directly by the parameters of their components.

A method of security evaluation of modular SNOW 2.0-like ciphers against correlation attacks over finite fields of characteristic 2 was further developed. In contrast to the known approaches of creating SNOW 2.0 correlation attacks, the developed method is based on analytical correlations obtained by the thesis, which summarize a number of separate results on matrix representations that are implementing by finite state machines. The developed method is applicable to modular SNOW 2.0-like ciphers and allows to obtain lower bounds of the efficiency of known correlation attacks directly by the parameters of the components of the encryption algorithm.

The practical significance of the obtained results consists in developing the software implementations that allow in real time to calculate the values of the lower bounds of the complexity and amount of material required to process any of the known correlative attacks on an arbitrary binary or modular SNOW 2.0-like cipher with 8 bit s-boxes. The developed programs are used to evaluate security of the cipher "Strumok", as well as its binary version. They can be used in practice to evaluate the security of other SNOW 2.0-like stream ciphers in SITS of Ukraine.

The scientific and practical results of the thesis were implemented at the Foreign Intelligence Service of Ukraine (in the research scientific work «Korifena») and in the scientific and technical developments of CJSC «Institute of Information Technologies».

Keywords: cybersecurity, correlation attack, cryptanalysis, security evaluation.

Список основних публікацій здобувача:

1. Олексійчук А.М., Поремський М.В. Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r. *Захист інформації.* 2017. Т. 19, № 2, с. 126-131.

2. Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки.* 2017. Випуск 15, с. 150-155.

3. Олексійчук А.М., Поремський М.В. Загальна схема побудови кореляційних атак на SNOW 2.0-подібні потокові шифри. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2018. Випуск 1 (32), с. 70-79.

4. Олексійчук А.М., Конюшок С.М., Поремський М.В. Обґрунтування стійкості потокового шифру «Струмок» відносно кореляційних атак над скінченними полями характеристики 2. *Математичне та комп'ютерне моделювання. Серія: Технічні науки.* 2019. Випуск 19, с. 114-119.

5. Alekseychuk A.N., Koniushok S.M., Poremskyi M.V. Upper Bounds on the Imbalance of Discrete Functions Implemented by Sequences of Finite Automata. *Cybernetics and Systems Analysis.* 2019. Volume 55, Issue 5, pp. 752-759.

6. Alekseychuk A.N., Koniushok S.M., Poremskyi M.V. A Method of Evaluating the Security of SNOW 2.0-Like Ciphers Against Correlation Attacks Over the Finite Extensions of Two Element Fiel. *Cybernetics and Systems Analysis*. 2020. Volume 56, Issue 1, pp. 40-52.

7. Олексійчук А.М., Поремський М.В. Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r // *III Міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки і захисту інформації».* 22-25 лютого 2017 р., К., 2017, с. 131.

8. Олексійчук А.М., Поремський М.В Застосування алгоритму BKW для побудови швидких кореляційних атак на словоорієнтовані потокові шифри. // *XIX міжнародна науково-технічна конференція «Безпека інформації в інформаційно-телекомунікаційних системах».* 25-26 лютого 2-17 р., К., 2017, с. 123-124.

9. Олексійчук А.М., Поремський М.В, Стрателюк Д.П. Кореляційні атаки на спрощені версії SNOW 2.0-подібних потокових шифрів // *XX міжнародна науково-технічна конференція «Безпека інформації в інформаційно-телекомунікаційних системах».* 22-24 травня 2018 р., К., 2018, с. 90.

10. Олексійчук А.М., Поремський М.В Метод обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полями порядку 2^r // *Науково-практичної конференція «Сучасні інформаційні технології та кібербезпека».* 15-16 листопада 2018 р., К., 2018, с. 41-43.

11. Поремський М.В. Експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість SNOW 2.0-подібних потокових шифрів відносно кореляційних атак // *Науково-практична конференція «Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання».* 19-20 листопада 2019 р., К., 2019, с. 37.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СІТС – спеціальна інформаційно-телекомунікаційна система;

ПШ – потоковий шифр;

ЛРЗ – лінійний регістр зсуву;

ОС – операційна система;

ПК – персональний комп’ютер;

СР – система рівнянь;

ВСТУП

Актуальність теми. Забезпечення інформаційної безпеки є вкрай важливим на даному етапі розвитку українською держави, що зумовлено великою кількістю зовнішніх та внутрішніх загроз. Серед найважливіших задач у сфері інформаційної безпеки держави, від вирішення яких залежать її економічна стабільність та суверенітет, є розробка нових та вдосконалення існуючих криптографічних систем і методів захисту інформації. На сьогодні криптографічні системи утворюють важливу складову сучасних спеціальних інформаційно-телекомунікаційних систем (СІТС). Основними вимогами до криптосистем є висока швидкодія при реалізаціях на різних обчислювальних платформах та стійкість, тобто спроможність протистояти усім відомим криптоаналітичним атакам. Це зумовлює, зокрема, широке використання потокових шифрів у сучасних захищених мережевих протоколах (шифр ChaCha20), стандартах мобільного зв'язку (шифри A5/1 та A5/2) та в апаратних застосуваннях з обмеженими ресурсами (шифр ACHTERBAHN-128/80). Поряд з цим, спостерігається значна зацікавленість потоковими шифрами у світовій спільноті, про що говорить проведення міжнародних конкурсів (NESSIE, eSTREAM), а також конкурсів в окремих країнах (CRYPTREC).

На сьогодні значна увага приділяється створенню та дослідженню криптографічних властивостей слово-орієнтованих ПШ, призначених для ефективної програмної реалізації на 32- або 64-розрядних процесорах. Важливий клас таких шифрів утворюють SNOW 2.0-подібні ПШ, прототипом яких є алгоритм потокового шифрування SNOW 2.0, що є на сьогодні міжнародним стандартом. Іншим прикладом SNOW 2.0-подібного шифру є нещодавно створений в Україні шифр "Струмок", прийнятий як національний стандарт ДСТУ 8845:2019. Невід'ємною частиною процесу створення таких

шифрів, що зумовлює вибір окремих компонент і параметрів для їх побудови, є обґрунтування їх стійкості відносно усіх відомих на сьогодні атак.

Аналіз доступних публікацій показує, що найбільш потужними атаками на SNOW 2.0 (складність яких може бути помітно менше складності повного перебору ключів) є кореляційні атаки, які базуються на побудові та розв'язанні систем лінійних рівнянь зі спотвореними правими частина над полями порядку 2^r, де $r \geq 2$. При цьому виявляється, що методи, розвинуті для оцінювання стійкості до таких атак саме шифру SNOW 2.0, стають незастосовними у випадку SNOW-2.0-подібних шифрів, які будуються над полями порядку 2^{64} або більше (наприклад, для шифру "Струмок"). В цілому, на сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість SNOW-2.0-подібних ПШ відносно відомих кореляційних атак безпосередньо за параметрами їх компонент.

Наведені факти свідчать про наявність певного протиріччя між потребами практики у сучасних SNOW 2.0-подібних потокових шифрах та відсутністю методів обґрунтування їх стійкості відносно відомих кореляційних атак. Зазначене протиріччя приводить до *наукової задачі, яка полягає у розробці методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак*, розв'язанню якої присвячено дану дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася в рамках розроблення та прийняття національного стандарту України ДСТУ 8845-2019 (шифр "Струмок"), виконання науково-дослідної роботи "Корифена" (номер держреєстрації 0118U001653) на замовлення Служби зовнішньої розвідки України та відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Мета та задачі досліджень. *Метою дисертаційної роботи є* усунення існуючого протиріччя між потребами у застосуванні в СІТС України сучасних SNOW 2.0-подібних потокових шифрів та відсутністю методів обґрунтування стійкості цих шифрів відносно відомих кореляційних атак.

Для досягнення поставленої мети **необхідно розв'язати такі окремі задачі дослідження:**

1. Провести аналіз відомих атак на SNOW 2.0-подібні потокові шифри, з'ясувати сутність та навести формальний опис відомих кореляційних атак над скінченними полями характеристики 2.

2. Отримати науково обґрунтовану аналітичну нижню оцінку інформаційної складності кореляційних атак над скінченними полями характеристики 2.

3. Отримати аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри; порівняти за трудомісткістю та обсягом матеріалу кореляційні атаки, що будуються над полями різних порядків.

4. Розробити метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2; отримати чисельні оцінки стійкості двійкових версій шифрів SNOW 2.0 та "Струмок" відносно відомих кореляційних атак; провести експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак.

5. Отримати аналітичні співвідношення та оцінки незбалансованості дискретних відображень, що реалізуються послідовностями скінченних автоматів; розробити метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2; отримати чисельні оцінки стійкості шифрів SNOW 2.0 та

“Струмок” відносно відомих кореляційних атак; провести експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак.

Об’єктом дослідження у дисертаційній роботі є процес перетворення інформації з використанням SNOW 2.0-подібних потокових шифрів, призначених для застосування в СІТС України, а *предметом дослідження* – методи обґрунтування стійкості зазначених шифрів відносно відомих кореляційних атак.

Методи дослідження. Основу дисертаційних досліджень складають теоретичні дослідження (математичні методи оцінювання стійкості потокових шифрів відносно кореляційних атак). Для розв’язання окремої задачі 2 використано методи теорії ймовірностей і теорії інформації. Задачу 3 розв’язано за допомогою методів теорії скінченних полів, лінійної алгебри та перетворення Фур’є псевдобулевих функцій, а задачі 4, 5 – з використанням методів лінійної алгебри, теорії ймовірностей і теорії скінченних автоматів. Експериментально-статистичні дослідження та чисельні розрахунки на ЕОМ виконувалися з використанням середовища розробки IntelliJ IDEA.

Наукова новизна отриманих результатів. Підсумком вирішення перелічених вище окремих задач є такі нові наукові результати, що висуваються на захист.

1. *Удосконалено* аналітичну оцінку інформаційної складності кореляційних атак на потокові шифри. На відміну від раніше відомої (евристичної) оцінки, отримана аналітична оцінка має належне наукове обґрунтування, містить явну залежність від ймовірності помилки атаки та є справедливою для будь-яких кореляційних атак на потокові шифри незалежно від способу побудови або методу розв’язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

2. *Вперше* отримано аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри. На відміну від відомих співвідношень, які визначають квадратичну евклідову незбалансованість, отримане співвідношення встановлює вираз цього параметра в термінах коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Це дозволяє отримувати нижні оцінки трудомісткості й обсягу матеріалу, потрібного для реалізації кореляційних атак на SNOW 2.0-подібні шифри та порівнювати за трудомісткістю та обсягом матеріалу кореляційні атаки, що будуються над полями різних порядків.

3. *Вперше* розроблено метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на полем з двох елементів, розроблений метод базується на отриманому дисертантом аналітичному співвідношенні для параметра, який характеризує ефективність атаки, та дозволяє обґрунтовувати стійкість двійкових SNOW 2.0-подібних потокових шифрів безпосередньо за параметрами їх компонент.

4. *Отримав подальший розвиток* метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на SNOW 2.0, розроблений метод базується на отриманих дисертантом аналітичних співвідношеннях, які узагальнюють низку окремих результатів про матричні представлення незбалансованості відображень, що реалізуються скінченними автоматами. Розроблений метод є застосовним до модулярних r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування.

Практичне значення отриманих результатів. Представлені в дисертаційній роботі нові наукові та практичні результати дозволяють:

– ввести науково обґрунтовані параметри вузлів заміни SNOW 2.0-подібних шифрів, що характеризують їх стійкість відносно відомих кореляційних атак;

– скоротити (не менш як у 2^{11} разів) час обчислення зазначених параметрів завдяки застосуванню розробленого дисертантом алгоритму;

– обґрунтувати практичну стійкість національного стандарту потокового шифрування України "Струмок" відносно відомих кореляційних атак (на рівні $2^{249,40}$ операцій за наявності не менше ніж $2^{249,38}$ знаків гами);

– підвищити обґрунтованість експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Дисертантом розроблено також комп'ютерні програми, які дозволяють в режимі реального часу обчислювати значення нижніх меж трудомісткості та обсягу матеріалу, потрібного для реалізації будь-якої з відомих кореляційних атак на довільний двійковий чи модулярний SNOW 2.0-подібний шифр, що використовує вузли заміни довжини 8 бітів. Розроблені програми застосовані для обґрунтування стійкості шифру "Струмок", а також його двійкової версії. Вони можуть бути використані на практиці при дослідженні стійкості інших SNOW 2.0-подібних потокових шифрів у СІТС України.

Наукові та практичні *результати дисертаційної роботи реалізовані* в Службі зовнішньої розвідки України – в результаті виконання НДР "Корифена" (акти від 13.02.2019) та в науково-технічних розробках ЗАО "Інститут інформаційних технологій" (акт від 26.09.2019).

Особистий внесок здобувача. У статті [1] та тезах доповіді [7] здобувачем отримано неасимптотичну нижню оцінку інформаційної складності кореляційних атак, які будуються шляхом розв'язання систем лінійних рівнянь

зі спотвореними правими частинами над скінченними полями характеристики 2, а у статті [2] – узагальнення цієї оцінки на випадок довільного скінченного кільця; у статті [3] та тезах доповідей [8, 9] дисертанту належить схема побудови кореляційних атак на SNOW 2.0-подібні ПШ за допомогою функціє сліду скінченного поля та метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над полями порядку 2^r; в [4] дисертантом запропоновано швидкий алгоритм обчислення параметрів вузлів заміни SNOW 2.0-подібних шифрів, що характеризують їх стійкість відносно кореляційних атак і отримано чисельні оцінки стійкості ПШ “Струмок”; в [5] дисертанту належать аналітичні співвідношення та оцінка для незбалансованості дискретного відображення, що реалізується послідовністю скінченних автоматів. Нарешті, у статі [6] та тезах доповіді [10] дисертантом отримано аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри, а також запропоновано метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над полями порядку 2^r.

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися на III Міжнародній науково-практичній конференції «Актуальні питання забезпечення кібербезпеки і захисту інформації» (смт. Верхнє Студене, 2017), XIX та XX міжнародних науково-технічних конференціях «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2017 – 2018), науково-практичній конференції «Сучасні інформаційні технології та кібербезпеки» (Київ, 2018), науково-практичній конференції “Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” (Київ , 2019).

Публікації. Основні наукові результати дисертаційної роботи опубліковано в 11 наукових працях: з них 6 наукових статей [1 – 6] в наукових фахових виданнях України та інших країн, 5 тез доповідей на наукових та науково-практичних конференціях [7 – 11].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації) і має 140 сторінок основного тексту, 12 рисунків, 6 таблиць, 10 сторінок додатків. Список використаних джерел містить 145 найменувань і займає 18 сторінок. Загальний обсяг дисертаційної роботи – 150 сторінок.

РОЗДІЛ 1

АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ ТА ОБҐРУНТУВАННЯ СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ ВІДНОСНО ВІДОМИХ АТАК

1.1. Аналіз ролі та значення сучасних потокових шифрів для систем захисту інформації у спеціальних інформаційних і телекомунікаційних системах

На сьогодні кіберпростір є невід'ємною частиною життя кожного громадянина України, що значною мірою впливає на економічний розвиток держави. Впровадження інтернет-технологій у державний сектор створює необхідність захисту інформації в спеціальних інформаційно-телекомунікаційних системах, а кібератаки, спрямовані на порушення роботи цих систем, становлять безпосередню загрозу економічній стабільності та суверенітету України.

Однією із основних задач кібербезспеки є кіберзахист. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [1] під кіберзахистом розуміється сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Очевидним є те, що криптографічні методи захисту інформації та криптосистеми є невід'ємною частиною організації кібербезпеки в Україні.

Основними вимогами до криптосистем є висока швидкодія при реалізаціях на різних обчислювальних платформах та стійкість, тобто спроможність

протистояти усім відомим криптоаналітичним атакам. Це зумовлює, зокрема, широке використання потокових шифрів у сучасних захищених мережевих протоколах (шифр ChaCha20 [2]), стандартах мобільного зв'язку (шифри A5/1 та A5/2 [3, 4]) та в апаратних застосуваннях з обмеженими ресурсами (шифр ACHTERBAHN-128/80 [5]). Поряд з цим, спостерігається значна зацікавленість у потокових шифрах з боку світової спільноти, про що свідчить проведення міжнародних конкурсів (NESSIE, eSTREAM), а також конкурсів в окремих країнах (CRYPTREC) [6 – 8]. Зауважимо, що протягом цих конкурсів запропоновано понад 50 алгоритмів потокового шифрування, а по завершенню конкурсів рекомендовано декілька ПШ, зокрема, Grain [9], HC-256 [10], Rabbit [11], Trivium [12], SOSEMANUK [13] та інші.

Історично перші реалізації потокових шифрів були біт-орієнтованими та розрахованими на швидку апаратну реалізацію, що зумовлює їх повільну швидкість роботи на сучасних процесорах [14]. З розробкою байт- та слово-орієнтованих ПШ стало можливим ефективно працювати на універсальних процесорах. Прикладами високошвидкісних слово-орієнтованих ПШ є SNOW 2.0 [15], SNOW 3G [16], SOBER [17], SOSEMANUK [13] та SNOW-V [18]. Шифри SNOW 2.0 та SNOW 3G є стандартизованими [19, 20], а шифри SOSEMANUK та SNOW-V розроблено на основі алгоритму SNOW 2.0.

З розвитком нових телекомунікаційних технологій вимоги до сучасних слово-орієнтованих ПШ зросли значною мірою. Зокрема, в [20] наведено стандарт шифрування SNOW 3G, який призначений для роботи з технологіями UMTS [21] та LTE [22] і розрахований на максимальну швидкість обробки інформації 9 Гбіт/с. Однак при переході на технологію 5G [18], орієнтовану на швидкість 20 Гбіт/с, він стає практично незастосовним. Поряд з цим сучасні версії слово-орієнтованих ПШ можуть досягати швидкостей понад 712 Гбіт/с, що принаймні в 14 разів перевищує швидкість роботи деяких сучасних блокових шифрів (наприклад, AES) [18]. Отже, на сьогодні є доцільним

використовувати слово-орієнтованих ПШ у системах, орієнтованих на програмну реалізацію, які задовольняють високими вимогами до швидкості обробки інформації.

Таким чином, поставлені нові вимоги до стійкості та швидкодії алгоритмів потокового шифрування свідчать про необхідність створення у Україні нового національного стандарту потокового шифрування. Порівняльні дослідження алгоритмів потокового шифрування [23] показують, що серед багатьох сучасних потокових шифрів найкращі результати демонструють шифри SNOW 2.0 та SOSEMANUK. Поряд з цим, шифр SNOW 2.0 є стандартизованим та одним із найбільш швидких програмно орієнтованих ПШ [15, 23]. Таким чином, цей шифр обрано як прототип нового національного стандарту потокового шифрування – "Струмок" [24, 25].

Алгоритми шифрування SNOW 2.0 та "Струмок" відносяться до класу SNOW 2.0-подібних потокових шифрів [26]. Кожен такий шифр є шифром імпульсного гамування та складається з генератора гами та алгоритму формування початкового стану генератора гами за ключем і вектором ініціалізації. Схеми генераторів гами шифрів SNOW 2.0 та "Струмок" наведено на рис. 1.1 та рис. 1.2 відповідно.

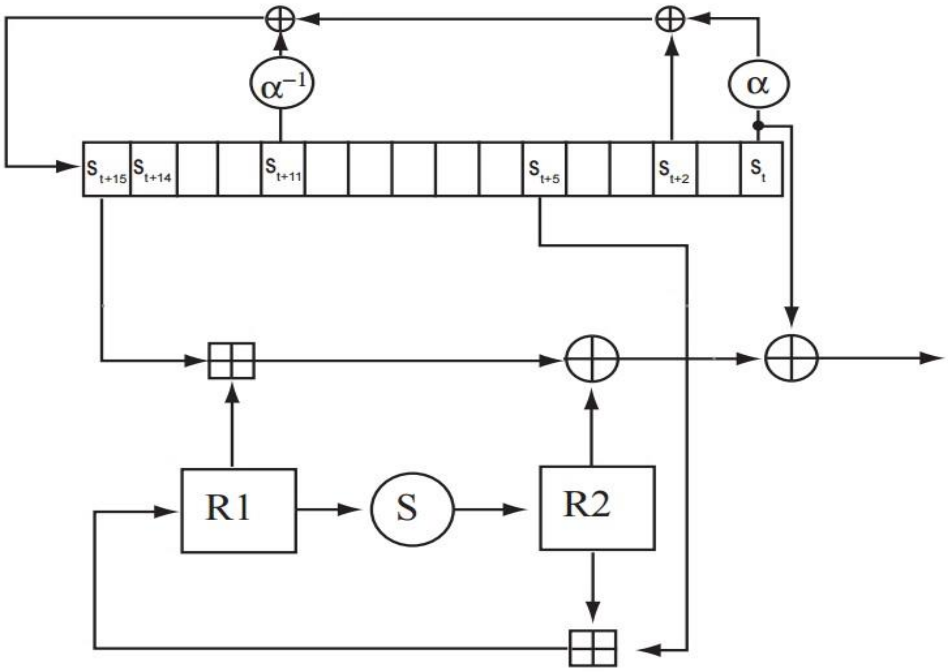

Рис. 1.1. Схема генератора гами шифру SNOW-2.0

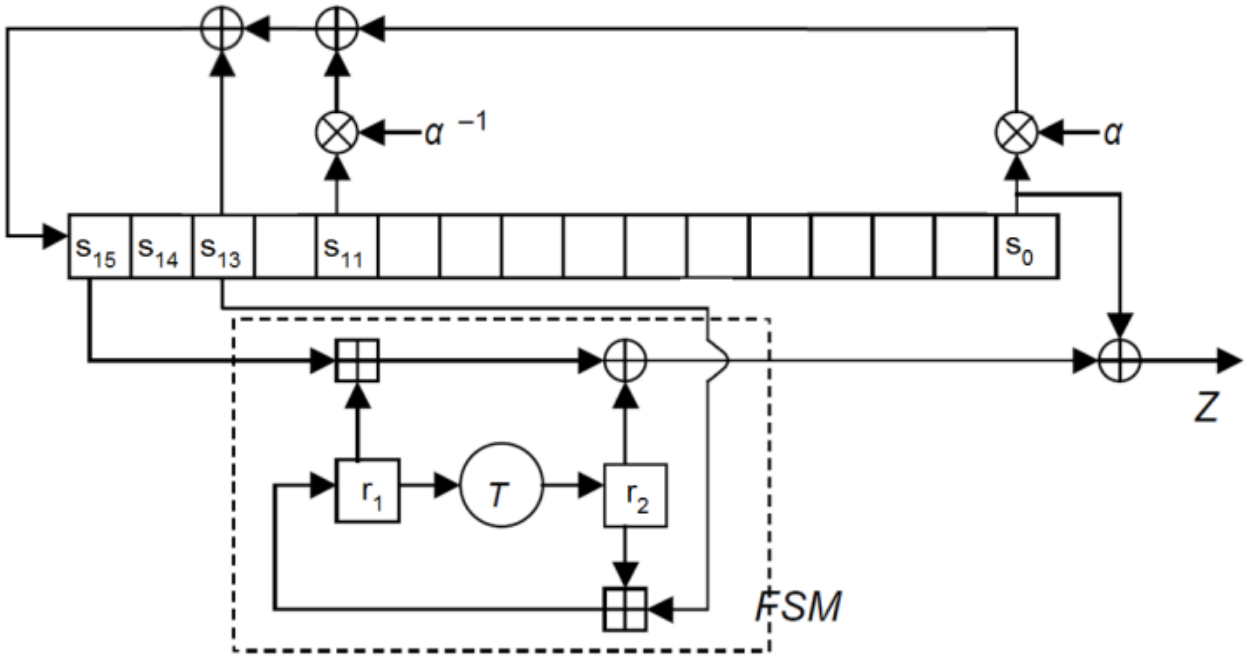

Рис. 1.2. Схема генератора гами шифру “Струмок”

Як зазначено вище, основним призначенням ПШ є забезпечення належної

стійкості, тому важливо вміти обґрунтовувати стійкість SNOW 2.0-подібних шифрів відносно усіх відомих атак. Особливо це стосується майбутнього національного стандарту потокового шифрування. Поряд з тим, як показано нижче, спроби застосувати відомі методи обґрунтування стійкості до шифру "Струмок" наштовхуються на труднощі, пов'язані з низкою невирішених задач. Для того щоб сформулювати ці задачі та проаналізувати способи подолання зазначених труднощів, треба розглянути основні моделі та означення потокових шифрів.

1.2. Математичні моделі синхронних потокових шифрів

На сьогодні переважну більшість сучасних потокових шифрів складають синхронні шифри імпульсного або модульного гамування. Кожен такий шифр визначається як сукупність двох алгоритмів [27, 28]:

1) генерації шифрувальної гами;

2) формування початкового стану генератора гами за ключем та вектором ініціалізації.

Як правило, останній алгоритм використовується також для реініціалізації початкового стану при фіксованій або вимушеній синхронізації шифраторів передачі та прийому інформації.

Стандартною математичною моделлю генератора гами є скінченний автономний автомат $\mathrm{A} = (S, Y, h, f)$, де S та Y позначають внутрішній і вихідний алфавіти автомата A відповідно, а $h : S \to S$ і $f : S \to Y$ є, відповідно, функціями переходів і виходів цього автомата [27]. Звичайно множини Y та S складаються з усіх двійкових векторів певної (не обов'язково однакової) довжини.

На рис. 1.3 показано процедури зашифрування та розшифрування двійкових повідомлень з використанням шифру гамування із генератором гами A. Спочатку за ключем k та вектором ініціалізації c у відповідності з певним алгоритмом F обчислюється початковий стан $x(0)$ автомату A: $x(0) = F(k, c)$, за яким далі формуються його внутрішня послідовність $\bar{x} = \{x(i) : i = 0,1, ...\}$ та шифрувальна гама $\bar{\gamma} = \{\gamma_i : i = 0,1, ...\}$, де $x(i+1) = h(x(i))$, $\gamma_i = f(x(i))$, $i = 0, 1, ...$ Символи t_i та s_i відкритого та, відповідно, шифрованого повідомлень у i-му такті шифрування пов'язані співвідношенням $s_i = t_i \oplus \gamma_i$, $i = 0, 1, ...$, де $\oplus$ позначає операцію додавання двійкових векторів за модулем 2.

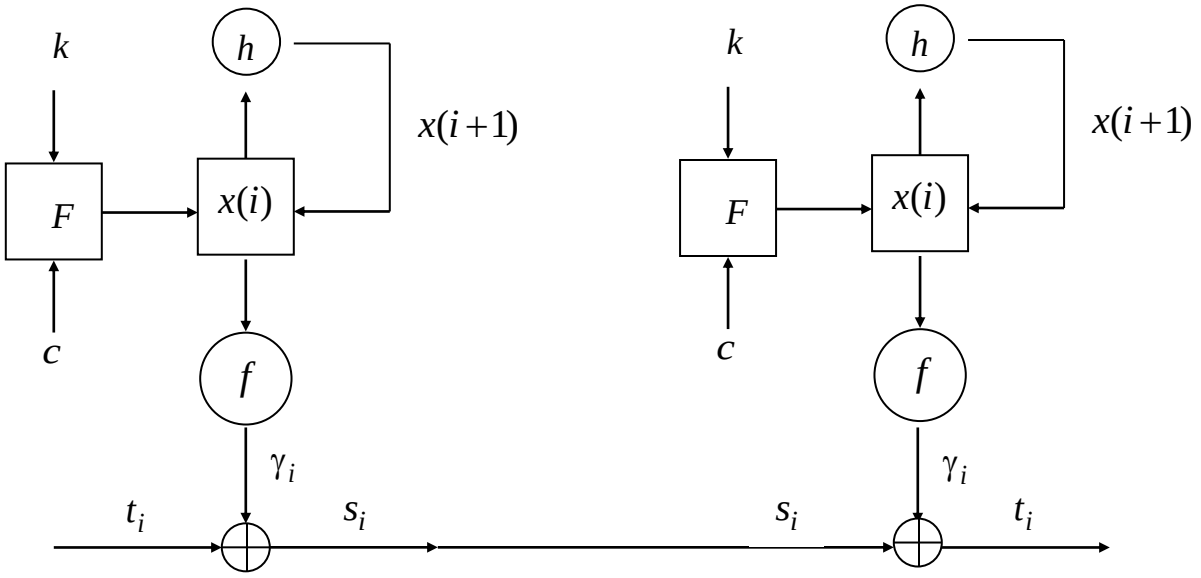

Рис. 1.3. Схематичне зображення процедур зашифрування/розшифрування повідомлень за допомогою потокового шифру

Традиційний метод синтезу генераторів гами полягає у побудові їх у вигляді послідовного з'єднання двох автоматів: генератора попередньої гами та блоку ускладнення. В ролі генераторів попередніх гам, як правило, використовуються лінійні регістри зсуву (ЛРЗ), які, за умови примітивності їх многочленів зворотного зв'язку, дозволяють отримувати псевдовипадкові

послідовності з гарними статистичними та структурними властивостями [27]. Призначення блоку ускладнення полягає у запобіганні простоти аналітичної (лінійної) залежності, що пов'язує знаки вихідної послідовності ЛРЗ з його початковим станом.

Як зазначено в підрозділі 1.1, починаючи з кінця 90-х років минулого століття, відбувається перехід від традиційних потокових шифрів, що будуються над полем з двох елементів, до слово-орієнтованих шифрів, які будуються над полями порядку 2^r, де $r \geq 2$. Останні включають, зокрема, клас SNOW 2.0-подібних потокових шифрів, до якого відносяться шифри SNOW 2.0 та "Струмок".

З метою подальшого аналізу відомих атак на зазначені шифри, наведемо їх формальне означення [26]. Позначимо V_m множину двійкових векторів довжини $m \geq 2$. Задамо на цій множині структуру поля порядку 2^m, узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Ототожнимо також звичайним чином елементи множини V_m з m-розрядними цілими числами та позначимо символом $+$ операцію додавання цих чисел за модулем 2^m.

Згідно з [26], вхідними даними для побудови SNOW 2.0-подібного потокового шифру з множиною ключів V_{l_0} та множиною векторів ініціалізації V_{l_1} є такі об'єкти:

– примітивний над полем F_{2^m} поліном $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus ... \oplus c_0$ степеня $n \geq 3$;

– натуральне число $\mu \in \overline{1, n-2}$;

– ін'єктивне афінне відображення $L : V_{l_0} \times V_{l_1} \to {V_m}^n$;

– підстановка $\sigma : V_m \to V_m$.

Задамо перетворення h та H на множині $V_m{}^n \times V_m{}^2$, вважаючи

$$h((x_{n-1}, x_{n-2}, \dots, x_0), u, v) = ((x_n, x_{n-1}, \dots, x_1), u', v')), \quad (1.1)$$

$$H((x_{n-1}, x_{n-2}, \dots, x_0), u, v) = ((x_n \oplus F, x_{n-1}, \dots, x_1), u', v')), \quad (1.2)$$

де

$$x_n = c_{n-1}x_{n-1} \oplus \dots \oplus c_0 x_0, \quad (1.3)$$

$$F = (x_{n-1} + u) \oplus v, \quad (1.4)$$

$$u' = x_\mu + v, \; v' = \sigma(u). \quad (1.5)$$

Зауважимо, що внаслідок нерівності $c_0 \neq 0$ (яка випливає з умови примітивності полінома $g(z)$) перетворення (1.1) і (1.2) є підстановками на множині $V_m{}^n \times V_m{}^2$.

За означенням SNOW 2.0-подібний потоковий шифр є шифром імпульсного гамування, який складається з генератора гами та алгоритму формування початкового стану генератора за ключем і вектором ініціалізації.

Генератор гами являє собою скінченний автономний автомат A з множиною внутрішніх станів $V_m{}^n \times V_m{}^2$, функцією переходів (1.1) та функцією виходів

$$f((x_{n-1}, x_{n-2}, \dots, x_0), u, v) = x_0 \oplus (x_{n-1} + u) \oplus v. \quad (1.6)$$

Алгоритм формування початкового стану генератора залежить від натурального параметра ν і складається з двох етапів:

1) формування за ключем $k \in V_{l_0}$ і вектором ініціалізації $c \in V_{l_1}$ стану $\iota_0 = (L(k,c), 0, 0)$ автомата A;

2) обчислення початкового стану генератора за формулою

$$s_0 = h(H^{\nu}(\iota_0)), \tag{1.7}$$

де H^{ν} позначає ν-й степінь відображення H відносно операції композиції.

Отже, на першому етапі за допомогою відображення L обчислюється вектор $L(k,c)$ довжини n над множиною V_m, який записується у накопичувач. Зазначений вектор, поряд з нульовими значеннями змінних u і v, утворює стан ι_0 автомата A. На другому етапі, згідно з формулою (1.7), обчислюється початковий стан $s_0 = ((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$. Далі автомат функціонує за законом $s_{i+1} = h(s_i)$, $\gamma_i = f(s_i)$, $i = 0, 1, \ldots$, проходячи послідовність станів $s_i = ((x_{i+n-1}, x_{i+n-2}, \ldots, x_i), u_i, v_i)$ та формуючи вихідну послідовність (шифрувальну гаму) γ_i, $i = 0, 1, \ldots$. Таким чином, стан генератора в i-му такті визначається за формулою

$$s_i = h^{i+1}(H^{\nu}(\iota_0)),\ i = 0, 1, \ldots, \tag{1.8}$$

а знак вихідної послідовності – за формулою

$$\gamma_i = x_i \oplus (x_{i+n-1} + u_i) \oplus v_i,\ i = 0, 1, \ldots. \tag{1.9}$$

Надалі вважатимемо, що $m = pt$, де $p,t \in \mathbf{N}$, $p,t \geq 2$, і підстановка σ має такий вигляд:

$$\sigma(x) = s(x)D = (s_1(x_1),...,s_p(x_p))D,\ x = (x_1,...,x_p) \in F_{2^t}^{\,p}, \qquad (1.10)$$

де s_i – підстановка (вузол заміни або s-блок) на множині V_t, яка ототожнюється з адитивною групою поля F_{2^t}, $i \in \overline{1,\ p}$, D – оборотна матриця порядку p над полем F_{2^t}.

Зауважимо, що у шифрі “Струмок” (рис. 1.2) використовуються такі параметри: $t = 8$, $p = 8$ $(m = 64)$, $n = 16$, $\mu = 13$, $\nu = 32$; підстановка σ має вигляд (1.10), де вузли заміни та матриця D задаються так само, як у блоковому шифрі “Калина” [29, 30]. При цьому довжина вектора ініціалізації дорівнює $l_1 = 256$, а довжина ключа може приймати одне з двох значень: $l_0 = 256$ або $l_0 = 512$. Нарешті, відображення L визначається таким чином:

1) якщо $l_0 = 256$, то

$$L(k_3,k_2,k_1,k_0,c_3,c_2,c_1,c_0) =$$

$$= (\underset{0}{k_3^{c_0}},\underset{1}{k_2},\underset{2}{k_1^{c_1}},\underset{3}{k_0^{c_2}},\underset{4}{k_3},\underset{5}{k_2^{c_3}},\underset{6}{\overline{k_1}},\underset{7}{\overline{k_0}},\underset{8}{k_3},\underset{9}{k_2},\underset{10}{\overline{k_1}},\underset{11}{k_0},\underset{12}{k_3},\underset{13}{\overline{k_2}},\underset{14}{k_1},\underset{15}{\overline{k_0}}),$$

де $k_i, c_i \in V_{64}$, $k^c \overset{\text{def}}{=} k \oplus c$, а $\overline{k}$ позначає вектор, який отримується шляхом інвертування усіх координат двійкового вектора k;

2) якщо $l_0 = 512$, то

$$L(k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$

$$= (\underset{0}{k_7^{c_0}}, \underset{1}{k_6}, \underset{2}{k_5}, \underset{3}{k_4^{c_1}}, \underset{4}{k_3}, \underset{5}{k_2^{c_2}}, \underset{6}{k_1}, \underset{7}{\overline{k_0}}, \underset{8}{k_4^{c_3}}, \underset{9}{\overline{k_6}}, \underset{10}{k_5}, \underset{11}{\overline{k_7}}, \underset{12}{k_3}, \underset{13}{k_2}, \underset{14}{\overline{k_1}}, \underset{15}{k_0}),$$

де $k_i, c_i \in V_{64}$, а символи k^c, $\overline{k}$ мають той самий сенс, що і вище [26].

1.3. Огляд відомих атак на SNOW 2.0-подібні потокові шифри

Сучасні методи криптоаналізу потокових шифрів, а також атаки, що будуються на їх основі, звичайно поділяють на методи “зламування”, спрямовані на відновлення ключів (або початкових станів генераторів гами), та методи, призначені для виявлення певних відмінностей між вихідними послідовностями генератора і суто випадковими послідовностями. При цьому в залежності від інформації, яка доступна криптоаналітику, та його можливостей криптоаналітичні атаки поділяють на такі класи (див., наприклад, [28]):

– атаки на основі відомого шифрованого тексту;

– атаки на основі відомого відкритого тексту (або гами, що виробляє генератор);

– атаки на основі відомих або підібраних векторів ініціалізації.

Крім перелічених видів атак, які проводяться за умови застосування єдиного невідомого ключа шифрування, розглядають також атаки зі зв’язаними ключами, при проведенні яких противник, маючи доступ до декількох шифрувальних перетворень, намагається відновити відповідні їм ключі, використовуючи певні відомі співвідношення між ними [31, 32]. Зауважимо також, що практична можливість здійснення атак на основі відомих або

підібраних векторів ініціалізації виникає внаслідок фіксованої або вимушеної синхронізації засобів шифрування [27, 28]. Практична стійкість відносно усіх цих видів атак є стандартною вимогою до сучасних потокових шифрів.

Іншою ознакою, за якою класифікуються криптоаналітичні атаки, є математичний апарат, що використовується при розв'язанні відповідної задачі криптоаналізу. Умовно відомі атаки можна поділити на методи опробування ключів, алгебраїчні та статистичні методи. Основним показником ефективності будь-якої атаки є її трудомісткість (або часова складність), що визначається як кількість тих чи інших операцій, необхідних для розв'язання задачі криптоаналізу з потрібною достовірністю. Оскільки трудомісткість, як правило, залежить від обсягу даних, потрібних для проведення атаки, то для характеристики її ефективності звичайно використовують ще один показник – інформаційну складність атаки, що визначається як найменший обсяг матеріалу, достатній її проведення з потрібною достовірністю.

На сьогодні відомо декілька видів атак, запропонованих на SNOW 2.0, які, в принципі, можуть бути застосовані до будь-якого SNOW 2.0-подібного потокового шифру (а також деяких інших потокових шифрів [16]). Це атаки зі зв'язаними ключами [32], узагальнена статистична атака та низка пов'язаних з нею атак [33 – 37], алгебраїчна атака [38] та широкий клас кореляційних атак [39 – 42].

Проаналізуємо докладніше умови, що визначають ефективність зазначених атак на SNOW 2.0-подібні потокові шифри.

1.3.1. Атаки зі зв'язаними ключами. Розглянемо означений вище SNOW 2.0-подібний шифр з множиною ключів V_{l_0} та множиною векторів ініціалізації V_{l_1}. Для будь-яких $k, k' \in V_{l_0}$, $c, c' \in V_{l_1}$, $r \in \overline{1,t}$ позначимо

$\iota_0 = (L(k,c), 0, 0)$, $\iota'_0 = (L(k',c'), 0, 0)$, $\iota_r = H^r(\iota_0)$, $\iota'_r = H^r(\iota'_0)$, де підстановка H визначається за формулою (1.2).

Згідно з [32, 43] пари (k,c) та (k',c') називаються еквівалентними із затримкою r (r-bits-phase shifting equivalent), якщо виконується рівність $\iota_r = \iota'_0$. Ключі k і k' називаються еквівалентними із затримкою r, якщо існують вектори ініціалізації $c,c' \in V_{l_1}$ такі, що пари (k,c) та (k',c') є еквівалентними із затримкою r.

Поняття еквівалентності із затримкою r має сенс для широкого класу потокових шифрів та означає, що стан генератора гами шифру в r-му такті, сформований за парою (k,c) при виконанні процедури ініціалізації, співпадає з початковим станом цього генератора, сформованим за іншою парою (k',c').

Наявність достатньо великої кількості ключів, еквівалентних із затримкою, дозволяє будувати на шифр атаки зі зв'язаними ключами (див. роботи [32, 43] та наведені в них посилання). Зокрема, для шифру SNOW 2.0 з довжиною ключа 256 біт існує 2^{192} пар ключів, еквівалентних із затримкою 4, що надає можливість побудувати на цей шифр атаку зі зв'язаними ключами, складність якої є величиною порядку 2^{67} [32].

В [26] показано, що стійкість будь-якого SNOW 2.0-подібного шифру відносно атак, що базуються на існуванні еквівалентних із затримкою r ключів, залежить від властивостей афінного відображення L та значення параметра $\lambda = n-1-\max\{\mu', \mu\}$, де $\mu' = \max\{ j \in \overline{0,n-1} : c_j \neq 0\}$, а μ визначається за формулою (1.5). При $r > \lambda$ тотожний збіг відрізків гами, отриманих при еквівалентних із затримкою r ключах та векторах ініціалізації, порушується, що виключає можливість проведення на шифр атак, аналогічних описаним в [32]. При $1 \le r \le \lambda$ відсутність еквівалентних із затримкою r ключів можна

забезпечити шляхом вибору відображення L, для якого існують так звані r-заборонені пари [26].

Отже, на підставі результатів [26] для обґрунтування стійкості SNOW 2.0-подібного шифру відносно атак зі зв'язаними ключами [32] достатньо переконатися у наявності заборонених пар відображення L, що можна зробити на практиці, виходячи з його означення. Зокрема, такі пари є для відображення, яке використовується у шифрі "Струмок" [26], що свідчить про стійкість цього шифру відносно атак з [32].

1.3.2. Узагальнена статистична атака. Ця атака запропонована в [36, 37] і являє собою узагальнення низки раніше відомих атак на основі підібраних векторів ініціалізації [33 – 35]. Метод оцінювання стійкості потокових шифрів відносно узагальненої статистичної атаки наведено у [44, 45].

Для будь-яких натуральних m,n позначимо $\mathbf{F}_2^{m\times n}$ множину матриць розміру $m\times n$ над полем $\mathbf{F}_2$, B_n – множину булевих функцій від n змінних, $d(f,g)=2^{-n}\,|\{x\in V_n : f(x)\neq g(x)\}|$ – відносну відстань між функціями $f,g\in B_n$.

Для означеного вище SNOW 2.0-подібного потокового шифру з множинами ключів та векторів ініціалізації V_{l_0} та V_{l_1} відповідно розглянемо довільну функцію $F=F(k,c)$, $k\in V_{l_0}$, $l\in V_{l_1}$ від $n=l_0+l_1$ змінних, задану за допомогою оракула, та зафіксуємо числа $s\in\overline{1,l_0-3}$ і $\theta\in(0,1)$.

За означенням [44] функція $g(k,c)=\varphi(kM_0,c)$, $k\in V_{l_0}$, $l\in V_{l_1}$ називається $(s+l_1)$-вимірним θ-допустимим наближенням функції F, якщо існують функція $\varphi\in B_{s+l_1}$ та матриця $M_0\in\mathbf{F}_2^{l_0\times s}$ такі, що $\mathrm{rank}(M_0)=s$ і $d(F,g)\le 1/2\cdot(1-\theta)$. Необхідною умовою застосовності узагальненої

статистичної атаки [36] є існування для функції-оракула F (яка задається за допомогою потокового шифру та допускає швидкий алгоритм обчислення) $(s+l_1)$-вимірних θ-допустимих наближень, де s є відносно невеликим числом ($s=20$), а θ є не надто близьким до 1 ($\theta=0{,}6$).

В [44, 45] показано, що застосування методу [36] до низки функцій-оракулів, які можуть бути використані для побудови узагальненої статистичної атаки на шифр SNOW-2.0, дає негативний результат. Зокрема, при $s \le 20$, $\theta=0{,}6$ з достовірністю не менше ніж $0{,}99$ жодна з зазначених функцій не має наближень, які знаходяться від неї на відносній відстані не більше ніж $1/2\cdot(1-\theta)=0{,}2$ та мають вигляд $\varphi(kM_0, c)$, $(k,c)\in V_{128}\times V_{128}$, де $\varphi: V_{148}\to\{0,1\}$, $M_0\in \mathbf{F}_2^{128\times 20}$. Це свідчить про практичну стійкість шифру відносно розглянутих варіантів узагальненої статистичної атаки.

Зауважимо, що, оскільки неможливо перебрати усі оракули-кандидати для застосування методу з [36], повне обґрунтування стійкості SNOW 2.0-подібних шифрів відносно узагальненої статистичної атаки потребує подальших досліджень. Поряд з тим, на сьогодні не відомо фактів, які свідчать про можливість успішного застосування цієї атаки (або низки подібних атак [33 – 35]) до шифру SNOW 2.0 чи інших аналогічних за будовою потокових шифрів [18].

1.3.3. Алгебраїчна атака. В [38] запропоновано алгебраїчну атаку на SNOW 2.0, яка, в принципі, є застосовною до будь-якого SNOW 2.0-подібного шифру.

Розглянемо потоковий шифр, означений в п. 1.2, що виробляє гаму γ_i, $i=0,1,\ldots$ за початковим станом $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$. Метою алгебраїчної атаки на цей шифр є відновлення значень $x_0, x_1, \ldots, x_{n-1}, v_0$ за послідовністю γ_i,

$i = 0, 1, \ldots$. Атака складається з двох етапів, на першому з яких формується певна система булевих рівнянь, що описує підстановку σ вигляду (1.10). Потім, на другому етапі будуються лінійні рівняння, які пов'язують знаки вихідної послідовності генератора з невідомими $x_0, x_1, \ldots, x_{n-1}, v_0$, а також додатковими змінними, які вводяться з метою лініаризації операції $+$ у виразах (1.4), (1.5). Далі отримана (нелінійна) система рівнянь розв'язується одним з відомих методів [38].

В [38] показано, що двійкова версія шифру SNOW 2.0, яка отримується шляхом заміни у схемі на рис. 1.1 операції додавання за модулем 2^{32} порозрядним булевим додаванням $\oplus$, може бути зламана за допомогою алгебраїчної атаки зі складністю порядку 2^{50} операцій за наявності приблизно 1000 знаків гами. Застосування атаки до оригінального алгоритму шифрування приводить до розв'язання системи, що складається з $156t$ квадратних рівнянь від $544 + 62t$ невідомих, де t дорівнює кількості доступних знаків гами. Оскільки на сьогодні не відомо методів розв'язання таких систем рівнянь, помітно більш ефективних за повний перебір, шифр SNOW 2.0 виявляється практично стійким відносно алгебраїчної атаки.

Аналіз цієї атаки показує, що при її застосуванні до будь-якого SNOW 2.0-подібного потокового шифру отримується аналогічна система рівнянь, степінь нелінійності яких співпадає з алгебраїчною імунністю підстановок s_i у формулі (1.10), $i \in \overline{1, p}$. Для шифру "Струмок" алгебраїчна імунність підстановок дорівнює 3 [29, 30], а число невідомих у системі є не менше ніж $64 \cdot 17 = 1088$, що свідчить про практичну стійкість цього шифру відносно атаки з [38].

1.3.4. Кореляційні атаки. Як відомо, сутність кореляційних атак на потокові шифри полягає у складанні та розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями або полями для

відновлення початкового стану генератора гами за його вихідною послідовністю [42, 46]. Такі атаки вважаються найбільш потужними з погляду трудомісткості та, як правило, є застосовними за менш жорстких умов щодо алгоритмів шифрування в порівнянні, наприклад, з алгебраїчними атаками.

Починаючи з роботи [47], до кінця 90-х років минулого століття запропоновано велику кількість різноманітних кореляційних атак на традиційні (двійкові) потокові шифри, перш за все, комбінувальні та фільтрувальні генератори гами [48 – 59]. Підсумки цього періоду розвитку кореляційних атак підбиті в роботі [46], де відзначено як здобуті досягнення, так і невирішені проблеми.

У [42, 56] описано певні кореляційні атаки, які базуються на розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над полями порядку 2^r, де $r \geq 2$, а у [60 – 70] – методи розв'язання зазначених систем над скінченними кільцями. Подібні кореляційні атаки вважаються більш ефективними в порівнянні з класичними атаками, які базуються на розв'язанні спотворених систем лінійних рівнянь над полем з двох елементів, проте низка важливих задач стосовно цих атак залишається невирішеною [71].

Кореляційні атаки на SNOW 2.0 [39 – 42, 72] утворюють єдиний з відомих класів атак, серед яких є суттєво більш ефективні в порівнянні з повним перебором ключів (за умови наявності достатньо великої кількості знаків гами; див. табл. 1.1).

Аналіз публікацій [39 – 42, 72] показує, що наведені в них кореляційні атаки базуються на тому, що сума знаків гами в будь-яких суміжних тактах є результатом спотворення знаку лінійної рекуренти з характеристичним многочленом того ж самого вигляду, що й многочлен зворотного зв'язку ЛРЗ на рис. 1.1.

Таблиця 1.1

Відомі кореляційні атаки на шифр SNOW 2.0

Атака	Вид атаки	Часова складність	Обсяг потрібного матеріалу
Watanabe et al., 2003 [72]	Розрізнювальна (над F_2)	2^{225}	2^{225}
Maximov-Johansson, 2005 [40]	Розрізнювальна (над $F_{2^{32}}$)	2^{202}	2^{202}
Nyberg-Wallen, 2006 [39]	Розрізнювальна (над F_2)	2^{174}	2^{174}
Lee et al., 2008 [41]	Відновлення початкового стану (над F_2)	$2^{198,77}$	$2^{212,38}$
ZXM, 2016 [42]	Відновлення початкового стану (над F_{2^8})	$2^{163,59}$	$2^{164,15}$

Для довільного SNOW 2.0-подібного шифру на підставі співвідношень (1.1), (1.5), (1.9) справедливі рівності

$$\gamma_i \oplus \gamma_{i+1} = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n} \oplus \xi_i,\ i = 0, 1, \ldots, \qquad (1.11)$$

де

$$\xi_i = ((x_{i+n-1} + u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus$$

$$\oplus ((x_{i+n} + x_{i+\mu} + v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i)),\ i = 0, 1, \ldots. \qquad (1.12)$$

Вважаючи, що змінні $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ у формулі (1.11) є незалежними випадковими величинами з рівномірним розподілом на множині V_m та виражаючи знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ лінійної рекуренти через початковий стан ЛРЗ, на підставі рівності (1.11) отримаємо систему лінійних

рівнянь зі спотвореними правими частинами над полем F_{2^m}, де спотворення є випадковими величинами (1.12).

Зазначену систему рівнянь можна розв'язувати безпосередньо, проте майже усі відомі кореляційні атаки на шифр SNOW 2.0 базуються на розв'язанні лише її наслідків над полями меншого порядку. Так, у [39, 41, 72] розглядаються булеві системи лінійних рівнянь зі спотвореними правими частинами, які отримуються з системи рівнянь (1.11) за допомогою певних лінійних перетворень, а в [42] – аналогічні системи лінійних рівнянь над полем порядку 2^8. Крім того, в [40] пропонується використовувати певні наслідки системи рівнянь (1.11) над полем порядку 2^{32} для побудови розрізнювальної атаки на SNOW 2.0. (Зазначимо, що найкраща на сьогодні кореляційна атака на SNOW 2.0 [42] потребує порядку $2^{163,59}$ таких рівнянь та має обчислювальну складність $2^{164,15}$).

Для оцінювання складності відомих алгоритмів розв'язання систем рівнянь вигляду (1.11) треба знати розподіл ймовірностей випадкових величин (1.12), проте при $m \geq 64$ найефективніші з відомих алгоритмів обчислення розподілів цього вигляду [40, 42] мають складність не менше ніж 2^{64} і є практично нереалізуємими. Дійсно, для обчислення усіх ймовірностей $\mathbf{P}(\xi_i = z)$, $z \in F_{2^m}$, необхідно виконати принаймні 2^m операцій та виділити такий самий обсяг пам'яті для їх зберігання.

В [39 – 41] побудовано кореляційні атаки над полем F_2, що полягають у розв'язанні спотворених систем рівнянь, які отримуються шляхом скалярного множення рівнянь (1.11) на булеві вектори α довжини m. При цьому використовуються швидкі алгоритми обчислення значень $(\mathbf{P}(\alpha\xi_i = 1) - 1)^2$, від яких залежить ефективність цих атак. Трудомісткість зазначених алгоритмів складає порядку 2^m операцій, отже, для обґрунтування стійкості шифру

відносно таких атак треба обчислити значення $(\mathbf{P}(\alpha\xi_i = 1) - 1)^2$ для усіх ненульових $\alpha \in V_m$, що потребує, принаймні, 2^{2m} операцій. (Зауважимо, що в [39 – 41] для побудови атак на SNOW 2.0, характеристики яких зазначені в табл. 1.1, вибираються конкретні вектори α малої ваги, які в цьому випадку неважко перебрати).

Аналогічні, але більш ефективні атаки запропоновано в [42], де розглядаються системи, що отримуються в результаті скалярного множення кожного рівняння системи (1.11) на вектор α довжини 4 над полем з 2^8 елементів ($m = 32 = 4 \cdot 8$). В [42] показано, що ефективність такої атаки визначається квадратичною евклідовою незбалансованістю розподілу ймовірностей $(p_\alpha(z) : z \in F_{2^8})$ спотворень у правих частинах рівнянь отриманої системи, тобто параметром $\Delta_\alpha = 2^{-8} \sum_{z \in F_{2^8}} (2^8 p_\alpha(z) - 1)^2$, який залежить від вектора α і може бути обчислений зі складністю приблизно 2^{32} операцій (для шифру SNOW 2.0). Зауважимо, що у випадку шифру “Струмок” обчислення аналогічного параметра за допомогою алгоритму з [42] потребує не менше ніж 2^{64} операцій; до того ж, для обґрунтування стійкості цього шифру відносно подібних атак треба перебрати $2^{64} - 1$ ненульових векторів α. Таким чином, безпосереднє застосування методів оцінювання ефективності кореляційних атак на SNOW 2.0 [39 – 42, 72] до шифру “Струмок” стає принципово неможливим.

Складність кореляційної атаки на будь-який потоковий шифр суттєво залежить від алгоритму розв’язання системи лінійних рівнянь зі спотвореними правими частинами, який використовується для проведення атаки. Ці алгоритми можна поділити на два класи: алгоритми розв’язання булевих СР, що використовують специфіку будови їх матриць коефіцієнтів; алгоритми

розв’язання довільних (не обов’язково булевих) СР з довільними матрицями коефіцієнтів.

На сьогодні відомо чимало алгоритмів з першого класу, розроблених для побудови швидких кореляційних атак на фільтрувальні або комбінувальні генератори гами. По суті, це – методи відновлення спотворених (або слабо спотворених) двійкових лінійних рекурент на основі застосування перевірочних співвідношень малої ваги [48, 49, 57], ітераційного декодування [49, 73, 74], загорткових кодів або турбоходів [79 – 78] та інші методи [50, 58, 59, 79, 80]. Як правило, їх ефективність суттєво залежить від кількості лінійних співвідношень малої ваги між рядками матриці коефіцієнтів системи, що розв’язується. Відомі оцінки часової складності зазначених алгоритмів, як правило, базуються на евристичних припущеннях (див., наприклад, [46]).

У випадку, коли матриця коефіцієнтів отриманої СР не має яскраво вираженої структури (тобто є подібною до випадкової рівноймовірної матриці), застосовуються алгоритми з другого класу. До них відносяться експоненційні алгоритми, що можуть бути використані для розв’язання слабоспотворених систем, які складаються з обмеженої (поліноміальної від числа невідомих) кількості рівнянь, або, більш ефективні, субекспоненційні алгоритми, використання яких є можливим за умови необмеженої кількості рівнянь (числа знаків гами, доступних криптоаналітику) [81 – 85].

На сьогодні найефективніші алгоритми розв’язання довільних систем лінійних рівнянь зі спотвореними правими частинами мають субекспоненційну часову складність і, як правило, базуються на розв’язанні задачі про адитивне представлення [85 – 88]. До них відносяться, зокрема, алгоритм BKW та його численні модифікації [81, 82, 85]. Саме такий алгоритм застосовується в [42] для побудови найшвидших з відомих сьогодні кореляційних атак на шифр SNOW 2.0.

Алгоритм з [42] складається з двох етапів, на першому з яких відбувається виключення певної кількості невідомих вхідної СР, що здійснюється шляхом додавань рівнянь вхідної системи з використанням алгоритму Вагнера [86]. Потім отримана спотворена система рівнянь від решти невідомих розв'язується методом максимальної правдоподібності з використанням швидкого перетворення Адамара.

В [42] отримано аналітичні оцінки часової складності зазначеного алгоритму та обсягу матеріалу, потрібного для його успішного застосування. Однак при цьому використовується евристичне припущення про те, що кількість рівнянь, потрібних для надійного розв'язання СР (від n_1 невідомих над полем порядку 2^r) на другому етапі алгоритму, складає $m \approx 2\Delta^{-1} n_1 r \ln 2$, де Δ є квадратичною евклідовою незбалансованістю розподілу спотворень у правих частинах рівнянь цієї системи. Зазначене припущення базується на неформальному застосуванні теореми кодування Шеннона, але його евристичний характер ставить під сумнів можливість використовувати наведені в [42] оцінки для обґрунтування стійкості SNOW 2.0-подібних шифрів відносно атак, що розглядаються.

Підсумовуючи сказане, слід констатувати, що на сьогодні відсутні методи обґрунтування стійкості довільних SNOW 2.0-подібних шифрів відносно відомих кореляційних атак безпосередньо за параметрами їх компонент. Спроба розповсюдити відомі методи оцінювання стійкості шифру SNOW 2.0 відноснокореляційних атак [39 – 42, 72] на деякі інші потокові шифри (наприклад, "Струмок") наштовхується на труднощі, пов'язані з розміром задач, які треба розв'язувати для отримання оцінок. Залишається також не вирішеною задача про обґрунтовану аналітичну оцінку інформаційної складності кореляційних атак на потокові шифри, тобто найменшого числа рівнянь у системі, що необхідно для її розв'язання із заданою достовірністю.

1.4. Основні напрями та окремі задачі дисертаційного дослідження

Вище показана актуальність *наукової задачі* дисертаційної роботи, яка полягає у розробці методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак.

Метою дисертаційної роботи є усунення існуючого протиріччя між потребами у застосуванні в СІТС України сучасних SNOW 2.0-подібних потокових шифрів та відсутністю методів обґрунтування стійкості цих шифрів відносно відомих кореляційних атак.

Об'єктом дослідження у дисертаційній роботі є процес перетворення інформації з використанням SNOW 2.0-подібних потокових шифрів, призначених для застосування в СІТС України, а предметом дослідження – методи обґрунтування стійкості зазначених шифрів відносно відомих кореляційних атак.

У відповідності до поставленої мети, наукова задача дисертаційної роботи включає в себе ряд взаємопов'язаних окремих задач, порядок розв'язання яких визначає основні напрями дисертаційних досліджень (рис. 1.4).

Перший напрям полягає в отриманні науково обґрунтованої аналітичної нижньої оцінки інформаційної складності кореляційних атак над скінченними полями характеристики 2, та в розрахунку аналітичного співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри (задачі 2 – 3 на рис. 1.4). Основною задачею *другого напряму* є розробка методів обґрунтування стійкості двійкових та модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2, а також розрахунок чисельних оцінок стійкості двійкових та модулярних версій шифрів SNOW 2.0 та "Струмок" відносно

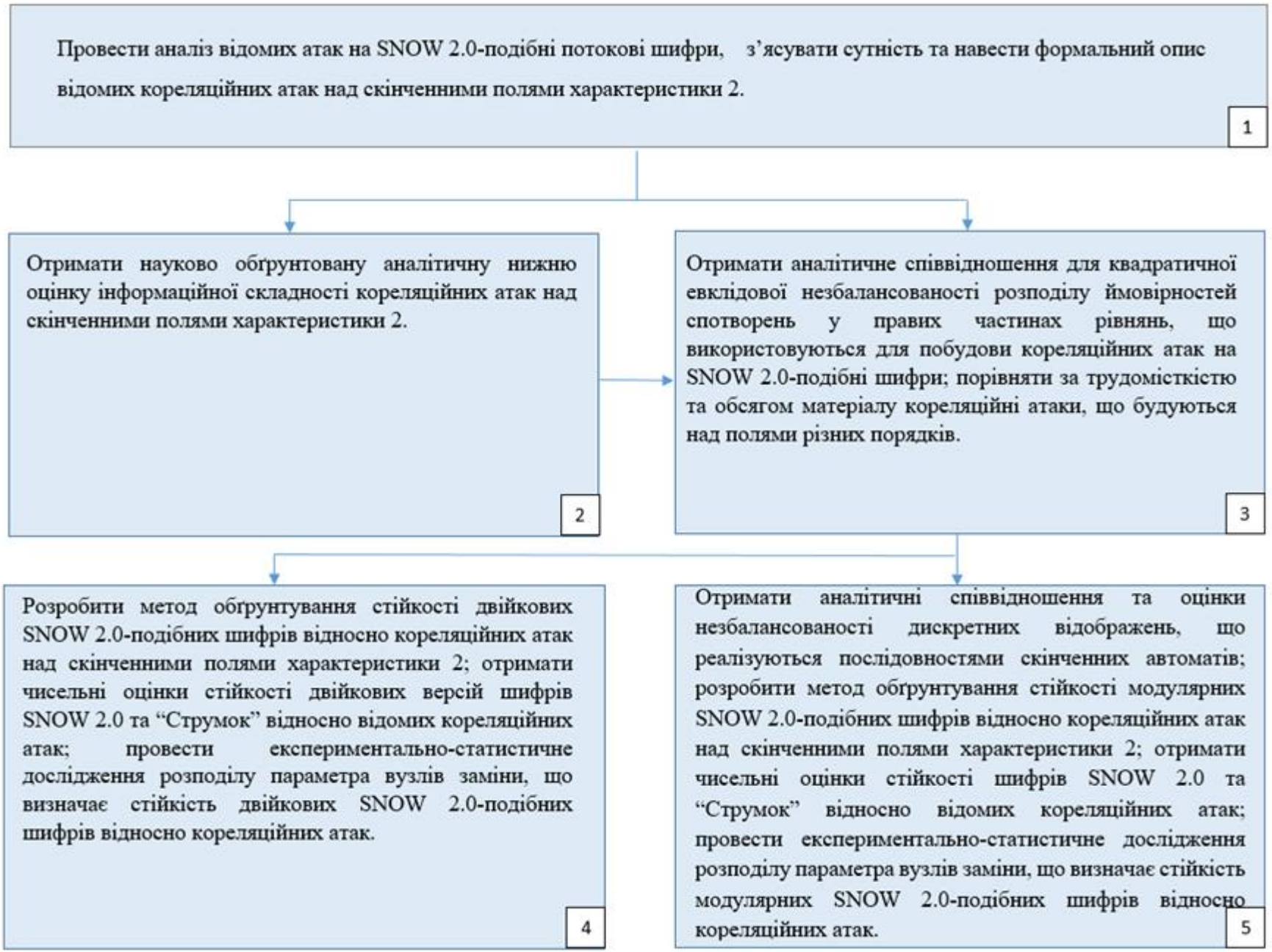

Рис. 1.4. Окремі задачі досліджень

Вирішення перелічених окремих задач дозволяє вирішити наукову задачу дисертаційної роботи та досягнути поставленої в роботі мети.

Висновки

1. З розвитком нових телекомунікаційних технологій значною мірою зростають вимоги до сучасних потокових шифрів, призначених для захисту інформації у спеціальних інформаційно-телекомунікаційних системах України. На сьогодні є доцільним використання слово-орієнтованих, зокрема, SNOW 2.0-пордібних ПШ у системах, призначених для програмної реалізації, які задовольняють високим вимогам до швидкості обробки інформації (понад 712 Гбіт/с). Порівняльні дослідження алгоритмів потокового шифрування показують, що одним з найкращих серед багатьох сучасних ПШ є шифр SNOW 2.0, який обрано як прототип нового національного стандарту потокового шифрування – шифру “Струмок”.

2. Кореляційні атаки на шифр SNOW 2.0 [39 – 42, 72] утворюють єдиний з відомих класів атак, серед яких є суттєво більш ефективні в порівнянні з повним перебором ключів. При цьому найкраща на сьогодні кореляційна атака на SNOW 2.0 [42] потребує порядку $2^{163,59}$ таких рівнянь та має обчислювальну складність $2^{164,15}$.

3. Спроба розповсюдити відомі методи оцінювання стійкості шифру SNOW 2.0 відносно кореляційних атак на деякі інші потокові шифри (наприклад, “Струмок”) наштовхується на труднощі, пов’язані з розміром задач, які треба розв’язувати для отримання оцінок. На сьогодні відсутні методи обґрунтування стійкості довільних SNOW 2.0-подібних шифрів відносно кореляційних атак безпосередньо за параметрами їх компонент.

4. Відомі аналітичні оцінки часової складності та обсягу матеріалу, потрібного для успішного застосування найкращої з відомих кореляційних атак на SNOW 2.0 [42] базуються на певному евристичному припущенні, що ставить під сумнів можливість використовувати ці оцінки для обґрунтування стійкості шифру SNOW 2.0 (а також подібних до нього шифрів) відносно кореляційних атак. Отже, залишається не вирішеною задача отримання науково обґрунтованих оцінок інформаційної складності кореляційних атак на SNOW 2.0-подібні потокові шифри.

Список використаних джерел у першому розділі

1. *Закон України «Про основні засади забезпечення кібербезпеки України»*. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.01.2020)

2. Daniel J. B. ChaCha, a variant of Salsa20. URL: https://cr.yp.to/chacha/chacha-20080128.pdf (дата звернення: 29.01.2020)

3. GSM System Security Study: Tehnical Information. URL: http://jya.com/gsm061088.htm (дата звернення: 29.01.2020)

4. Anderson R., Roe M. A5 The GSM Encryption Algorithm. URL: http://jya.com/crack-a5.htm (дата звернення: 28.01.2020)

5. Gammel B.M., Gottfert R., Kniffler O. Achterbahn-128/80. URL: http://www.matpack.de/achterbahn/Gammel_Goettfert_Kniffler_Achterbahn-128-80.pdf (дата звернення: 27.01.2020)

6. NESSIE: New European Schemes for Signatures, Integrity, and Encryption. URL: https://www.cosic.esat.kuleuven.be/nessie/ (дата звернення: 29.01.2020)

7. ECRYPT: The home page eSTREAM, the ECRYPT Stream Cipher Project. URL: http://www.ecrypt.eu.org/stream (дата звернення: 29.01.2020)

8. Biryukov A. Block Ciphers and Stream Ciphers: The State of the Art. URL: https://www.researchgate.net/publication/2895551_Block_Ciphers_and_Stream_Ciphers_The_State_of_the_Art (дата звернення: 29.01.2020)

9. Hell M., Johansson T., Maximov A. A Stream Cipher Proposal: Grain-128. URL: https://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain128_p3.pdf (дата звернення: 26.01.2020)

10. Wu H. Stream Cipher HC-256. URL: https://www.ecrypt.eu.org/stream/p3ciphers/hc/hc256_p3.pdf (дата звернення: 29.01.2020)

11. Vesterager M., Pedersen T., Christiansen J., Scavenius O. Rabbit: A new High-Performance Stream Cipher. *International Workshop on Fast Software Encryption*. 2003. P. 307-329.

12. De Canniere Ch., Preneel B. Trivium specifications. *eSTREAM, ECRYPT Stream Cipher Project*. 2006.

13. Berbain C., Billet O., Canteaut A. Sosemanuk, a fast software-oriented stream cipher. URL: https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/sosemanuk.pdf (дата звернення: 29.01.2020)

14. Дирда О. Метод побудови високошвидкісного програмно-орієнтованого потокового шифру. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник.* 2008. №. 2(17). С. 75-83

15. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. Selected Areas in Cryptography. *SAC 2002. LNCS 2295. Springer-Verlag*. P. 47 – 61

16. Li W. X., Lui F. Study and Realization of SNOW 3G in LTE System. *Advanced Materials Research*. Vol.756-759. P. 841-845 doi: 10.4028/www.scientific.net/AMR.756-759.841 (дата звернення: 03.02.2020)

17. Rose G. SOBER: A Stream Cipher based on Linear Feedback over GF (28). Unpublished report, QUALCOMM Australia. 1998

18. Ekdahl P., Johansson T., Maximov A. A new SNOW stream cipher called SNOW-V. URL: https://eprint.iacr.org/2018/1143.pdf (дата звернення: 26.01.2020)

19. ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers. 2011.

20. ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers. 2011. 92 p.

21. Weidel R. The UMTS (Universal Mobile Telecom Standard) Physical Layer Basics, Standard, and Frontend Matters. Andreas Springer. 2002

22. ETSI TS 136 101 V10.3.0. Technical specification. URL: https://www.etsi.org/deliver/etsi_ts/136100_136199/136101/10.03.00_60/ts_136101v100300p.pdf (дата звернення: 28.01.2020)

23. Кузнецов О.О., Іваненко Д.В., Луценко М.С. Порівняльні дослідження алгоритмів потокового криптографічного перетворення. *Радіотехніка*. 2007. № 119. С. 52-15.

24. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies*. 2018. P. 292 – 299.

25. *ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення*. 2019

26. Олексійчук А.М. Достатня умова стійкості SNOW 2.0-подібних потокових шфирів відносно певник атак зі зв'язани ключами. *Захист інформації*. 2016. Т. 18. № 3. С. 261 – 268.

27. Фомичев В.М. Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ. 2003. 400 с.

28. Katz J., Lindell Y. Introduction to modern cryptography. Chapman & Hall/CRC. 2014. 603p.

29. Oliynykov R.V. et. al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. URL: http://eprint.iacr.org/ 2015/650.pdf (дата звернення: 28.01.2020)

30. Олійников Р.В. та ін. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України. *Захист інформації*. 2015. Т. 17. № 2. С. 142 – 157.

31. Biham E. New types of cryptoanalytic attacks using related keys. *Advances in Cryptology – EUROCRYPT'93, Proceedings.* Springer-Verlag. 1993. P. 340 – 357.

32. Kircanski A., Youssef A., On the sliding property of SNOW 3G and SNOW 2.0. *IET Information Security*. 2011. Vol. 5. № 4. P. 199 – 206.

33. Fischer S., Khazaei S., Meier W. Chosen IV statistical analysis for key recovery attacks on stream ciphers. *AFRICACRYPT 2008, Proceedings.* Springer-Verlag, 2008. P. 236 – 245.

34. Saarinen Markku-Juhani O. Chosen-IV Statistical Attacks on eSTREAM Stream Ciphers. URL: https://www.ecrypt.eu.org/stream/papersdir/2006/013.pdf (дата звернення: 28.01.2020)

35. Englund H., Johansson T., Turan M. A Framework for Chosen IV Statistical Analysis of Stream Ciphers. *INDOCRYPT 2007: Progress in Cryptology*. 2007. P. 268-281.

36. Олексійчук А.М., Конюшок С.М., Сторожук А.Ю. Узагальнена статистична атака на синхронні потокові шифри. *Захист інформації*. 2015. Т. 17. № 3. С. 54 – 65.

37. Сторожук А.Ю. Модифицированная атака на фильтрующий генератор гаммы с линейным законом реинициализации и функцией усложнения близкой к алгебраически вырожденной. *Тези доповідей XVI міжнародної науково-практичної конференції ["Безопасность информации в информационно-телекоммуникационных системах"] (Київ, 21-24 травня 2013 р.)*. К.: ООО "ИП ЭДЕЛЬВЕЙС", НИЦ "ТЕЗИС" НТУУ "КПИ", 2013. С. 40 – 41.

38. Billet O., Gilbert H. Resistance of SNOW 2.0 against algebraic attacks. *Advanced in Cryptology – CT-RSA2005. LNCS3376. Springer-Verlag*. 2005. P. 19 – 28.

39. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption – FSE 2006*. *LNCS 4047*. *Springer-Verlag*. 2006. P. 144 – 162.

40. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology – ASIACRYPT 2005*. *LNCS 3788*. *Springer-Verlag*. 2005. P. 313 – 332.

41. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology – ASIACRYPT 2008*. *LNCS 5350*. *Springer-Verlag*. 2008. P. 524 – 538.

42. *Zhang B., Xu C., Meier W.* Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. URL: http://eprint.iacr.org/2016/311 (дата звернення: 28.01.2020)

43. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G security, V3.1.1: «Specification of the 3GPP Confidentiality and Integrity Algorithms: Document 2: KASUMI Specification». 2001.

44. Олексійчук А.М., Конюшок С.М., Сторожук А.Ю. Метод пошуку алгебраїчно вироджених наближень булевих функцій для побудови статистичних атак на синхронні потокові шифри. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2016. №. 1 (31) 2016. С. 65 – 79.

45. Сторожук А.Ю. «*Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій*», Дисертація на здобуття наукового ступеня кандидата технічних наук, URL: http://er.nau.edu.ua/bitstream/NAU/25171/1/dissert_Storozhuk.pdf (дата звернення: 28.01.2020)

46. Canteaut A. Fast correlation attacks against stream ciphers and related open problems, *The 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, ITW 2005, E-Proc.* 2005. P. 49-54.

47. Siegenthaler T. Correlation immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory 30*. 1984. pp. 776-780.

48. Canteaut A., Trabbia M. Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5. *Proceedings of Eurocrypt 2000*. *LNCS 1807*. 2000. P. 573-588.

49. Chose Ph., Joux A., Mitton M. Fast correlation attacks: an algorithmic point of view. *Proceedings of Eurocrypt 2002*. *LNCS 2332*. 2002. P. 209-221.

50. Coppersmith D., Halevi S., Jutla Ch. Cryptanalysis of stream ciphers with linear masking. *Proceedings of Crypto 2002*. *LNCS 2442*. 2002. P. 515-532. URL: http://eprint.iacr.org/2002/020 (дата звернення: 28.01.2020)

51. Golić J. Linear models for keystream generators, *IEEE Trans. on Computers*. № 45. 1996. P. 41-49.

52. Golić J. Correlation properties of a general binary combiner with memory. *Journal of Cryptology*. № 9 1996. P. 111-126.

53. Golić J., Bagini V., Morgari G. Linear cryptanalysis of Bluetooth stream cipher. *Proceedings of Eurocrypt 2002*. *LNCS 2332*. 2002. P. 238-255.

54. Johansson J., Joensson F. Fast correlation attacks through reconstruction of linear polynomials. *Proceedings of Crypto'2000*. *LNCS 1880*. 2000. P. 300-315.

55. Joensson F., Johansson T. A fast correlation attack on LILI-128. *Inf. Process. Lett.* № 81(3). 2002. P. 127-132.

56. Joensson F. Some results on fast correlation attacks. *Thesis, Lund University, Sweden*.

57. Meier W., Staffelbach O. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*. № 1. 1989. P. 159-176.

58. Meier W., Staffelbach O. Correlation properties of combiners with memory in stream ciphers. *Journal of Cryptology*. № 5. 1992. P. 67-86.

59. Mihaljevi M., Fossorier M., Imai H. Fast correlation attack algorithm with list decoding and an application. *Proceedings of Fast Software Encryption 2001. LNCS 2355*. 2002. P. 196-210.

60. Алексейчук А.Н. Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. № 4. 2001. С. 12-19.

61. Алексейчук А.Н., Лукъянов В.В. Метод декодирования блоковых кодов в канале с аддитивным по модулю 2^N шумом по частично известным входным и выходным сообщениям. *Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ НАН України*. №. 10. 2001. С. 88-93.

62. Балакин Г.В. Оценка истинного решения системы уравнений над кольцом вычетов при аддитивной помехе. *Проблемы теоретической кибернетики: Тез. докл. XII Междунар. конф. 1999 г. Нижний Новгород*. 1999. С. 15.

63. Алексейчук А.Н., Игнатенко С.М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольом вычетов по модулю 2^N. *Збірник наукових праць ІПМЕ НАН України*, № 20. 2003. С. 40-48.

64. Алексейчук А.Н., Игнатенко С.М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Реєстрація, зберігання і обробка даних.* № 1, Т. 7. 2005. С. 11-23.

65. Игнатенко С.М. Модификация метода максимума правдоподобия решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації.* № 1. 2007. С. 63-72.

66. Игнатенко С.М., Алексейчук А.Н. Алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N с использованием быстрого преобразования Ферма. *Тез. докл. VI Междунар.*

Научно-практич. Конф. «Безопасность информации в информационно-телекоммуникационніх системах». Киев. 2003. С. 42-43.

67. Игнатенко С.М., Алексейчук А.Н. Итеративный алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N. *Тез. докл. VIII Междунар. Научно-практич. Конф. «Безопасность информации в информационно-телекоммуникационніх системах».* Киев. 2005. С. 46-47.

68. Игнатенко С.М., Алексейчук А.Н. Быстрый алгоритм восстановления искаженных линейных рекуррентных последовательностей над кольцом вычетов по модулю 2^N. *Тез. докл. X Междунар. Научно-практич. Конф. «Безопасность информации в информационно-телекоммуникационніх системах».* Киев. 2007. С. 36-37.

69. Алексейчук А.Н., Игнатенко С.М., Конюшок С.Н. Быстрая корреляционная атака на генераторы гаммы над кольцом вычетов по модулю 2^N. *Праці міжнародного симпозіуму «Питання оптимізації обчислень (ПОО-XXXV)».* Україна, Крим, Велика Ялта, смт. Кацивелі. 2009. С. 14-18.

70. Ігнатенко С.М., Олексійчук С.М. Послідовна статистична атака на шифросистему LPN-C над кільцем лишків за модулем 2^N. *Тези доповідей XX Ювілейної Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах».* м. Буча Київської обл. 2018. С. 35-36.

71. Meier W. Fast correlation attacks: methods and countermeasures. *LNCS, FSE'2011, Proceedings, Springer Verlag*. 2011. P. 55-67.

72. Watanabe D., Biryukov A., de Cannière C. A distinguishing attack of SNOW 2.0 with linear masking method. *Selected Arreas in Cryptography – SAC 2003. LNCS 3006. Springer-Verlag*. 2003. P. 222 – 233.

73. Armknecht F. Improving fast algebraic attacks. *Fast Software Encryption. – FSE'04, Proceedings. – Springer-Verlag*. 2004. P.65 – 82.

74. Chepyzhov V., Johansson T., Smeets B. A simple algorithm for fast correlation attacks on stream ciphers. *Fast Software Encryption. – FSE'00, Proceedings. Springer*. 2000. P. 181 – 195.

75. Johansson T., Joensson F. Improved fast correlation attack on stream ciphers via convolutional codes. *Advances in Cryptology – EUROCYPT'99, Proceedings. Springer-Verlag*. 1999. P. 347 – 362.

76. Johansson T., Joensson F. Fast correlation attacks based on Turbo Code techniques. *Advances in Cryptology – CRYPTO'99, Proceedings. Springer-Verlag*. 1999. P. 181 – 197.

77. Johansson T., Joensson F. Theoretical analysis of a correlation attack based on convolutional codes. *IEEE Transactions on Information Theory*. 2002. Vol. 48, № 8. P. 2173 – 2181.

78. Johannesson R., Zigangirov K. Fundamentals of convolutional coding. *IEEE Press*. 1999. 442 P.

79. Lee S., Chee S., Park S., Park S. Conditional correlation attack on non linear filter generators. *Advances in Cryptology – ASIACRYPT'96, Proceedings. Springer-Verlag*. 1996. P. 360 – 367.

80. Golić J. Correlation properties of a general binary combiner with memory. *Journal of Cryptology*. 1996. Vol. 9, № 2. P. 111 – 126.

81. Bogos S. LPN in cryptography: an algorithmic study. PhD thesis. *Ecole Polytechnique Federale de Lausanne*. 2017. URL: https://infoscience.epfl.ch/record/228977/files/EPFL_TH7800.pdf (дата звернення: 28.01.2020)

82. Levieil E., Fouque P.-A. An Improved LPN Algorithm. *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings, LNCS, Springer*. Vol. 4116. 2006. P. 348-359.

83. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA*. 2005. P. 84-93.

84. Олексійчук А.М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. *Прикладная радиоэлектроника.* 2012. Т. 11, № 2. С. 3-11.

85. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. Vol. 50, № 3. 2003. P. 506-519.

86. Wagner D. A generalized birthday problem. *Advances in Cryptography – CRYPTO'02, Processing. Springer Verlag.* 2002. P. 288-303.

87. Minder L., Sinclair A. The extended k-tree algorithm. *The 19th Annual ACM-SIAM Sympposium on Discrete Algorithms, Proceedings.* 2009. P. 586-595.

88. Bhattacharyya A., Indyk P., Woodruff D.P. The complexity of linear dependence problems in vector spaces. *Innovation is computer science – ICS*. 2010. P. 496-508.

РОЗДІЛ 2

АНАЛІТИЧНІ ВИРАЗИ ТА ОЦІНКИ ПАРАМЕТРІВ, ЩО ВИЗНАЧАЮТЬ СТІЙКІСТЬ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК

У розділі 1 зазначено, що найбільш потужними з відомих атак на шифр SNOW 2.0 [1, 2] є кореляційні атаки, сутність яких полягає у складанні та розв'язанні систем лінійних рівнянь зі спотвореними правими частинами, зокрема, систем рівнянь над полями порядку більшого ніж 2 [3 – 7]. Не дивлячись на певний прогрес у цьому напрямі, залишаються не вирішеними задачі, пов'язані з розробкою методів оцінювання та обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак. На сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість зазначених шифрів відносно відомих кореляційних атак безпосередньо за параметрами їх компонент. Крім того, спроба розповсюдити відомі методи оцінювання стійкості SNOW 2.0 відносно кореляційних атак на деякі інші потокові шифри (наприклад, "Струмок" [8], який є стандартизованим в Україні алгоритмом потокового шифрування [9]) наштовхується на труднощі, пов'язані з розміром задач, які треба розв'язувати для отримання оцінок. На відміну від SNOW 2.0, побудованого над полем порядку 2^{32}, шифр "Струмок" задається над полем порядку 2^{64}, що призводить до неможливості практичного застосування певних алгоритмів [4, 5, 7], складність яких збільшується від $2^{32} \div 2^{37}$ до 2^{64} двійкових операцій.

В даному розділі викладено нові результати, які складають наукову основу розроблених дисертантом методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно широкого класу кореляційних атак.

В п. 2.1 наведено означення SNOW 2.0-подібних потокових шифрів та низки пов'язаних з ними понять. Зауважимо, що в дисертаційній роботі досліджуються шифри більш загального вигляду в порівнянні з запропонованими в [10]. Зокрема, визначаються двійкові шифри, які відрізняються від раніше означених (модулярних) шифрів [10] заміною операції додавання за модулем степеня двійки порозрядним булевим додаванням двійкових векторів. Двійкові шифри можуть розглядатися як спрощені версії відповідних модулярних шифрів (до яких відносяться SNOW 2.0 і "Струмок"), проте їх дослідження становить самостійних інтерес.

В п. 2.2, базуючись на роботі [7], описано клас атак, які розглядаються в подальшому. На відміну від [7], для опису цих атак (а точніше, систем рівнянь зі спотвореними правими частинами, до розв'язання яких зводяться зазначені атаки) використовується функція сліду скінченного поля у його підполе. Це надає можливість отримати більш корисний для подальшого аналізу опис, зокрема, встановити аналітичний вираз параметра, який визначає ефективність кореляційної атаки в термінах коефіцієнтів Фур'є розподілу спотворень у правих частинах відповідної системи рівнянь.

В п. 2.3 отримано неасимптотичну нижню оцінку інформаційної складності кореляційних атак, які базуються на розв'язані систем лінійних рівнянь зі спотвореними правими частинами над довільними скінченними полями характеристики 2. Отримана (науково обґрунтована) оцінка уточнює раніше відому (евристичну) оцінку інформаційної складності [7] та є справедливою для будь-яких кореляційних атак на довільні потокові шифри незалежно від способу побудови або методу розв'язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

В п. 2.4 доведено твердження, яке дозволяє звести задачу отримання нижніх оцінок трудомісткості кореляційної атаки з визначеного класу та обсягу матеріалу, потрібного для її успішної реалізації, до побудови верхніх меж максимуму модулів коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Зазначене твердження встановлює аналітичний вираз параметра, від якого безпосередньо залежить стійкість SNOW 2.0-подібних потокових шифрів відносно зазначених кореляційних атак, і являє собою основний науковий результат цього розділу.

Нарешті, в п. 2.5 досліджено взаємозв'язок між ефективністю атак над полями порядку $2^{r'}$, де $r' > 1$, та звичайних, двійкових атак, що будуються над полем з двох елементів. Показано, що перехід від двійкових кореляційних атак до атак над полями порядку $2^{r'}$ може підвищити ефективність перших не більше ніж в $2^{r'}$ разів.

Зауважимо, що окремі наукові результати цього розділу, зокрема, викладені в п. 2.3 і 2.4, є застосовними не тільки до SNOW 2.0-подібних шифрів і можуть бути використані для розв'язання інших задач кореляційного криптоаналізу симетричних шифросистем.

2.1. SNOW 2.0-подібні потокові шифри

Для будь-якого натурального r позначимо V_r множину двійкових векторів довжини r. Задамо на цій множині структуру поля F_{2^r} (порядку 2^r), узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Ототожнимо елементи множини V_r з r-розрядними цілими числами, вважаючи, що вектору $x = (x_1, x_2, \dots, x_r) \in V_r$ відповідає число

$x_1 + 2x_2 + \cdots + 2^{r-1}x_r$, та позначимо символом $\overset{r}{+}$ операцію додавання цих чисел за модулем 2^r.

За означенням вхідними даними для побудови *генератора гами SNOW 2.0-подібного потокового шифру* є такі об'єкти (рис. 2.1):

– примітивний многочлен $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ над полем F_{2^r};

– підстановка $\sigma : V_r \to V_r$;

– натуральне число $\mu \in \overline{1, n-2}$;

– комутативна групова операція $*$ на множині V_r.

Генератор гами являє собою скінченний автономний автомат з множиною внутрішніх станів $V_r{}^n \times V_r{}^2$, функцією переходів

$$h((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n, x_{n-1}, \ldots, x_1), x_\mu * v, \sigma(u)),$$

та функцією виходів

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus (x_{n-1} * u) \oplus v,$$

де $x_0, \ldots, x_{n-1}, u, v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0$. Отже, знак гами в i-му такті визначається за початковим станом $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$ генератора за допомогою рекурентних співвідношень

$$\gamma_i = x_i \oplus (x_{i+n-1} * u_i) \oplus v_i, \qquad (2.1)$$

$$u_{i+1} = x_{i+\mu} * v_i,\ v_{i+1} = \sigma(u_i), \tag{2.2}$$

справедливих для усіх $i = 0, 1, \ldots$.

В подальшому, як правило, розглядаються SNOW 2.0-подібні потокові шифри, що задовольняють умові $* \in \{\oplus, \overset{r}{+}\}$. При цьому шифр називається *двійковим*, якщо $* = \oplus$ та *модулярним*, якщо $* = \overset{r}{+}$, де $r \geq 2$.

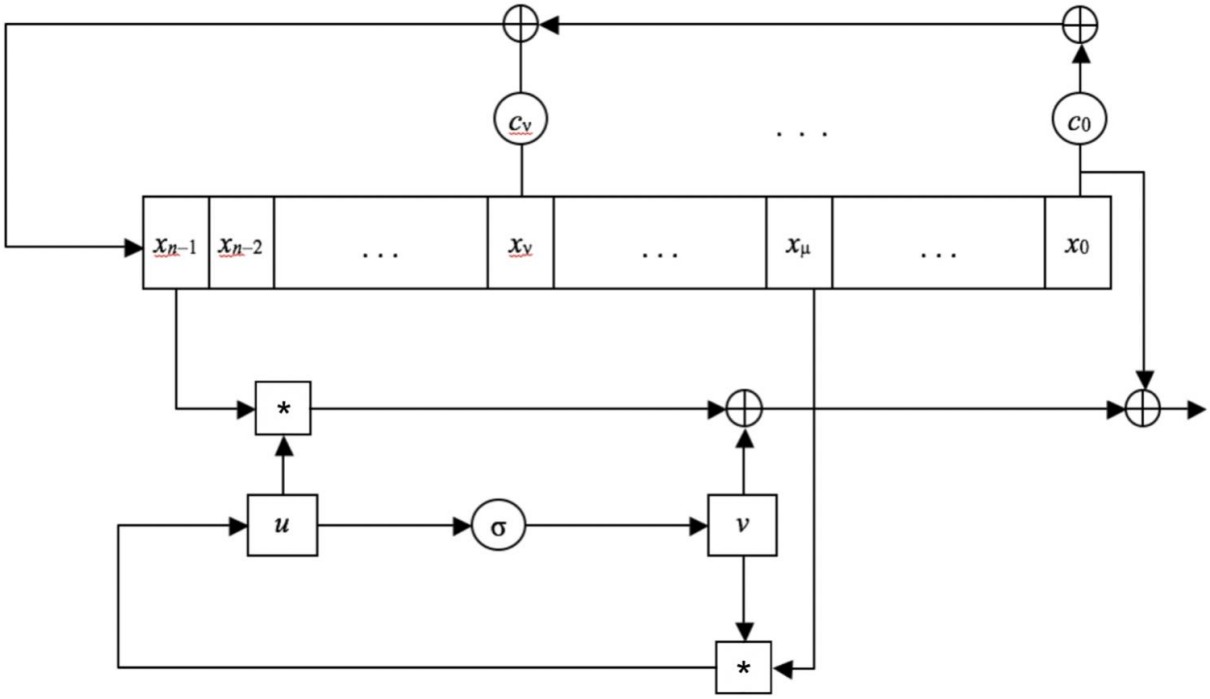

Рис. 2.1. Схема генератора гами SNOW 2.0-подібного потокового шифру

SNOW 2.0-подібний шифр називається *ординарним*, якщо існують цілі числа $p, t \geq 2$ такі, що $r = pt$, базис B поля F_{2^r} над підполем F_{2^t}, підстановки $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0, p-1}$, та оборотна $p \times p$-матриця D над полем F_{2^t} такі, що

при ототожненні елементів z та $\sigma(z)$ поля F_{2^r} з наборами їх координат в базисі B виконується рівність

$$\sigma(z) = (s_0(z_0),...,s_{p-1}(z_{p-1}))D,\ z = (z_0,...,z_{p-1}) \in F_{2^t}^p. \qquad (2.3)$$

Звичайно підстановки $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0,\ p-1}$, називаються *вузлами заміни* або s-*блоками* шифру, що розглядається.

Приклад 2.1. SNOW 2.0 [1] є ординарним модулярним шифром з параметрами $t = 8$, $p = 4$ ($r = 32$). При цьому $n = 16$, $\mu = 5$, а підстановки s_i, $i \in \overline{0,\ p-1}$, та матриця D задаються так само, як у раундовому перетворенні блокового шифру Rijndael [11].

Приклад 2.2. Потоковий шифр "Струмок" [8] є ординарним модулярним SNOW 2.0-подібним шифром з параметрами $t = 8$, $p = 8$ ($r = 64$). При цьому $n = 16$, $\mu = 13$, а підстановки s_i, $i \in \overline{0,\ p-1}$, та матриця D задаються так само, як у блоковому шифрі "Калина" [12, 13].

2.2. Кореляційні атаки на SNOW 2.0-подібні потокові шифри

Як зазначено в розділі 1, практично всі відомі кореляційні атаки на SNOW 2.0 [3 – 7] базуються на тому, що сума знаків шифрувальної гами в будь-яких суміжних тактах є результатом спотворення знаку лінійної рекуренти над полем F_{2^r}, за якою можна безпосередньо відновити початковий стан ЛРЗ генератора. Для довільного SNOW 2.0-подібного потокового шифру на підставі співвідношень (2.1), (2.2) справедливі рівності

$$\gamma_i \oplus \gamma_{i+1} = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n} \oplus \xi_i,\ i = 0, 1, \ldots, \qquad (2.4)$$

де

$$\xi_i = ((x_{i+n-1} * u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus$$

$$\oplus ((x_{i+n} * x_{i+\mu} * v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i)),\ i = 0, 1, \ldots. \qquad (2.5)$$

Вважаючи, що змінні $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ у формулі (2.5) є незалежними випадковими величинами з рівномірним розподілом на множині V_r та виражаючи знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ лінійної рекуренти через початковий ЛРЗ на рис. 2.1, отримаємо систему (2.4) лінійних рівнянь зі спотвореними правими частинами над полем F_{2^r}, де спотворення є випадковими величинами (2.5).

Опишемо метод побудови наслідків системи (2.4), які використовуються далі для побудови кореляційних атак на SNOW 2.0-подібні потокові шифри.

Запишемо перші N рівнянь СР (2.4) у вигляді

$$b_i = A_i a \oplus \xi_i,\ i \in \overline{0, N-1}, \qquad (2.6)$$

де $b_i = \gamma_i \oplus \gamma_{i+1}$, $A_i a = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n}$, A_i – відомий вектор-рядок довжини n над полем F_{2^r}, $a = (x_0, \ldots, x_{n-1})^{\mathrm{T}}$ – невідомий вектор-стовпець, що дорівнює початковому стану ЛРЗ генератора на рис. 2.1.

Зафіксуємо довільний (натуральний) дільник r' числа r та позначимо $\mathrm{Tr}_{2^{r'}}^{2^r}(z) = z \oplus z^{2^{r'}} \oplus \cdots \oplus z^{2^{r'(r''-1)}}$ слід елемента $z \in F_{2^r}$ в полі $F_{2^{r'}}$, де $r'r'' = r$.

Нагадаємо (див., наприклад, [14], означення 2.30), що базиси $\mathrm{B} = \{b_1, ..., b_{r''}\}$ і $\hat{\mathrm{B}} = \{\hat{b}_1, ..., \hat{b}_{r''}\}$ поля F_{2^r} над підполем $F_{2^{r'}}$ називаються *дуальними*, якщо $\mathrm{Tr}_{2^{r'}}^{2^r}(b_i \hat{b}_j) = 1$ при $i = j$, $\mathrm{Tr}_{2^{r'}}^{2^r}(b_i \hat{b}_j) = 0$ – у протилежному випадку. З даного означення випливає, що слід добутку довільних елементів поля F_{2^r} співпадає зі скалярним добутком векторів їх координат у (будь-яких) дуальних базисах.

Для побудови системи-наслідку СР (2.6) зафіксуємо елемент $c \in F_{2^r} \setminus \{0\}$ та пару дуальних базисів B і $\hat{\mathrm{B}}$ поля F_{2^r} над підполем $F_{2^{r'}}$. Помітимо, що з рівностей (2.6) випливають рівності $\mathrm{Tr}_{2^{r'}}^{2^r}(cb_i) = \mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca)) \oplus \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$, $i \in \overline{0, N-1}$, причому $\mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca))$ є скалярним добутком векторів A_i' та a' над полем $F_{2^{r'}}$, які отримуються в результаті заміни кожної координати вектора A_i (відповідно, вектора ca) її представленням у базисі B (відповідно, у базисі $\hat{\mathrm{B}}$). Звідси випливає, що вектор $a' \in F_{2^{r'}}^{nr''}$ співпадає с істинним розв'язком системи рівнянь зі спотвореними правими частинами

$$A_i' x = b_i' = A_i' a' \oplus \eta_i, \; i \in \overline{0, N-1}, \tag{2.7}$$

де $b_i' = \mathrm{Tr}_{2^{r'}}^{2^r}(cb_i)$, $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$ для кожного $i \in \overline{0, N-1}$.

Таким чином, для відновлення вектора a з системи рівнянь (2.4) достатньо побудувати для заздалегідь вибраних дільника r' числа r та елемента $c \in F_{2^r} \setminus \{0\}$ систему рівнянь (2.7) над полем $F_{2^{r'}}$ та відновити її істинний розв'язок a' одним з відомих методів. Знаючи вектор a' та базис $\hat{\mathrm{B}}$, можна отримати вектор ca, а отже, і шуканий вектор a.

Зауважимо, що всі відомі кореляційні атаки на шифр SNOW 2.0 базуються на розв'язанні систем рівнянь зазначеного вигляду (проте без явного використання функції сліду) або наслідків таких СР, які складаються з лінійних комбінацій їх окремих рівнянь. Зокрема, в [3, 4, 6] розглядаються булеві системи лінійних рівнянь зі спотвореними правими частинами ($r' = 1$), які отримуються з СР (2.4) за допомогою певних лінійних перетворень над полем F_2, а в [7] – аналогічні системи рівнянь над полем порядку 2^8 ($r' = 8$). Крім того, в [5] пропонується використовувати безпосередньо СР (2.4) над полем порядку 2^{32} для побудови розрізнювальної атаки на SNOW 2.0.

Опишемо докладніше *алгоритм розв'язання СР зі спотвореними правими частинами вигляду* (2.7), який використовується при проведенні кореляційних атак. Як зазначено в розділі 1, на сьогодні відомо чимало субекспоненційних алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полем з двох елементів (див., наприклад, [7, 15 – 17]), причому деякі з них допускають природні узагальнення на випадок СР над скінченними полями характеристики 2 або навіть над довільними скінченними кільцями [18].

Надалі вважатимемо, що при проведенні кореляційної атаки на SNOW 2.0-подібний шифр для розв'язання СР (3.7) використовується один з найшвидших на сьогодні алгоритмів, який запропоновано в [7].

Зазначений алгоритм залежить від параметрів $k \geq 2$, що є степенем двійки, та $l' \in \overline{1, l}$, де $l = nr''$, і складається з двох етапів.

На першому етапі за допомогою k-алгоритму Вагнера (k-tree algorithm) [19] здійснюється виключення з вхідної СР (2.7) останніх $l - l'$ невідомих. В результаті отримується нова СР зі спотвореними правими частинами від l' невідомих над полем $F_{2^{r'}}$, кожне рівняння якої є сумою певних k рівнянь вхідної СР. На другому етапі отримана СР розв'язується методом максимальної правдоподібності із застосуванням швидкого перетворення Адамара.

Таким чином, зазначений алгоритм дозволяє відновити перші l' невідомих системи рівнянь (2.7). Застосовуючи його $\lceil l/l' \rceil$ разів до різних наборів невідомих, що не перетинаються, можна знайти шуканий вектор a'.

Зауважимо, що розподіл спотворень η_i у правих частинах рівнянь системи (2.7) має такий вигляд:

$$\mathbf{P}\{\eta_i = z\} \quad = \sum_{x \in F_{2^r}:\ \mathrm{Tr}_{2^{r'}}^{2^r}(cx)=z} \mathbf{P}\{\xi_i = x\},\ z \in F_{2^{r'}}, \tag{2.8}$$

де випадкова величина ξ_i визначається за формулою (2.5), $i \in \overline{0, N-1}$. Крім того, спотворення у правій частині кожного рівняння системи, яка отримується в результаті виконання першого етапу алгоритму, є сумою k незалежних випадкових величин, розподілених за законом (2.8). Отже, розподіл спотворень у правих частинах рівнянь системи, отриманої після першого етапу, має такий вигляд:

$$p_{c,r',k}(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\},\ z \in F_{2^{r'}}. \tag{2.9}$$

Зауважимо також, що зазначені спотворення є залежними випадковими величинами, проте в [7] (неявно) використовується евристичне припущення про їх незалежність. Для оцінки кількості рівнянь, потрібних для надійного розв'язання СР на другому етапі алгоритму, використовується евристична формула [7]:

$$m_{c,r'}(k, l') \approx 2\Delta_{c,r'}(k)^{-1} l' r' \ln 2, \tag{2.10}$$

де

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} p_{c,r',k}(z) - 1)^2 . \qquad (2.11)$$

При цьому, згідно з [7], середня трудомісткість алгоритму розв'язання СР (2.7) (за умови незалежного випадкового та рівноймовірного вибору рядків A'_i, $i \in \overline{0, N-1}$) визначається за формулою

$$T_{c,r'}(k,l') = (m_{c,r'}(k,l'))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{c,r'}(k,l') + r'l'2^{r'l'}) + 2^{r'(l'+1)}, \qquad (2.12)$$

а обсяг матеріалу, потрібного для успішного розв'язання цієї СР – за формулою

$$N = N_{c,r'}(k,l') = k 2^{\frac{r'(l-l')}{\theta}} (2l'r' \ln 2)^{\frac{1}{\theta}} \Delta_{c,r'}(k)^{-\frac{1}{\theta}}, \qquad (2.13)$$

де $\theta = 1 + \log k$. Зрозуміло, що для підвищення ефективності алгоритму параметри k та l' слід вибирати, виходячи з умови мінімальності значення (2.12).

2.3. Обґрунтована нижня оцінка інформаційної складності кореляційних атак над полями порядку 2^r

Евристичний характер формули (2.10) ставить під питання можливість застосовувати співвідношення (2.12), (2.13) для отримання обґрунтованих нижніх меж часової складності та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на SNOW 2.0-подібні потокові шифри. Дійсно, формула (2.10) базується на евристичних міркуваннях (див. [7], теор. 5) і надає

інформацію про наближене значення інформаційної складності атаки (тобто кількості рівнянь, потрібних для надійного розв'язання СР на другому етапі наведеного вище алгоритму).

Основним науковим результатом цього підрозділу є обґрунтована неасимптотична нижня оцінка інформаційної складності атаки, що базується на розв'язані системи лінійних рівнянь зі спотвореними правими частинами над полем порядку 2^r. Отримана оцінка є справедливою для будь-яких кореляційних атак на довільні потокові шифри незалежно від способу побудови (або методу розв'язання) системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

Уточнімо постановку задачі, яка розв'язується нижче.

Розглянемо систему рівнянь зі спотвореними правими частинами

$$Ax = b, \tag{2.14}$$

де A – $m \times n$-матриця над полем F_q, $q = 2^r$, b – вектор довжини m з координатами

$$b_i = A_i a \oplus \xi_i, \; i \in \overline{1,m}, \tag{2.15}$$

де $A_1, \ldots, A_m$ – рядки матриці A, $a = (a_1, \ldots, a_n)^{\mathrm{T}}$ – невідомий вектор над полем F_q (істинний розв'язок СР (2.1)), $\xi_1, \ldots, \xi_m$ – незалежні випадкові величини, розподілені за законом $\mathbf{P}\{\xi_i = z\} = p(z)$, де $p(z) \geq 0$ для кожного $z \in F_q$, $\sum_{z \in F_q} p(z) = 1$. Далі вважатимемо, що стовпці матриці A є лінійно незалежними векторами над полем F_q. Задача розв'язання СР (2.14) полягає у відновленні

вектора a за відомими матрицею A, вектором b і розподілом ймовірностей $p_\xi = (p(z) : z \in F_q)$.

Припустимо, що матриця A є фіксованою. В цьому випадку будь-який алгоритм відновлення вектора a з системи рівнянь (2.14) задається певним відображенням $D_A : F_q^{\,m} \to F_q^{\,n}$, яке ставить у відповідність вектору b з координатами (2.15) "оцінку" вектора a. При цьому (середня) ймовірність помилки алгоритму визначається за формулою $\delta(D_A) = q^{-n} \sum_{a \in F_q^{\,n}} \mathbf{P}\{D_A(b) \neq a\}$.

Нагадаємо (див. підрозділ 1.3), що для будь-якого $\delta \in (0, 1/2)$ інформаційна складність атаки, яка базується на розв'язанні СР вигляду (2.14), визначається як найменше число m рівнянь у системі, для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж δ. Іншими словами, інформаційна складність – це найменший обсяг матеріалу, необхідного для відновлення вектора a з ймовірністю не менше ніж $1 - \delta$.

В [7] (теор. 5) наведено евристичну (наближену) оцінку інформаційної складності кореляційних атак, що базуються на розв'язанні СР вигляду (2.14):

$$m \approx \frac{2nr}{\Delta(p_\xi)} \ln 2, \tag{2.16}$$

де

$$\Delta(p_\xi) = q^{-1} \sum_{z \in F_q} (qp(z) - 1)^2 . \tag{2.17}$$

Зауважимо, що параметр (2.17) називається *квадратичною евклідовою незбалансованістю* розподілу ймовірностей $p_\xi = (p(z) : z \in F_q)$ [7].

Наступне твердження уточнює оцінку (2.16).

Твердження 2.1. Нехай m є найменшим числом рівнянь у системі (2.14), для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$. Тоді

$$m \geq \frac{nr(1-\delta) - h(\delta)}{\Delta(p_\xi)} \ln 2, \tag{2.18}$$

де $\Delta(p_\xi)$ визначається за формулою (2.17), $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$.

Доведення. Помітимо, що вектор b з координатами (2.15) є результатом передачі випадкового повідомлення Aa (де вектор a має рівномірний розподіл на множині $F_q^{\,n}$) дискретним симетричним каналом без пам'яті, а саме, каналом з адитивним шумом на групі $(F_q, +)$. Пропускна здатність такого каналу дорівнює $C_\xi = \log_2 q - H(p_\xi) = r - H(p_\xi)$, де $H(p_\xi) = -\sum_{z \in R} p(z) \log_2 p(z)$ – ентропія розподілу p_ξ [20], с. 118.

Розглянемо довільне відображення $D_A : F_q^{\,m} \to F_q^{\,n}$ таке, що $\delta(D_A) \leq \delta$. На підставі відомих властивостей взаємної інформації та ентропії (див., наприклад, [20], с. 22), а також лінійної незалежності стовпців матриці A над полем F_q справедливі такі співвідношення:

$$nr - H(Aa / D_A(b)) = H(Aa) - H(Aa / D_A(b)) = I(Aa; D_A(b)) \leq$$

$$\leq I(Aa; b) \leq mC_\xi = m(r - H(p_\xi)).$$

З іншого боку, використовуючи нерівність Фано [29], с. 142, отримаємо, що

$$H(Aa / D_A(b)) \le \delta(D_A(b))(n\log q - 1) + h(\delta(D_A(b))) \le \delta nr + h(\delta).$$

Отже, справедлива нерівність

$$nr - \delta nr + h(\delta) \le m(r - H(p_\xi)). \tag{2.19}$$

Нарешті, використовуючи оцінку $\ln x \le x - 1,\ x > 0$, отримаємо, що

$$r - H(p_\xi) = (\ln 2)^{-1} \sum_{z \in F_q} p(z) \ln(qp(z)) \le (\ln 2)^{-1} \sum_{z \in F_q} p(z)(qp(z) - 1).$$

$$\le (\ln 2)^{-1} \sum_{z \in F_q} p(z)(qp(z) - 1) = (\ln 2)^{-1} \Delta(p_\xi). \tag{2.20}$$

Безпосередньо з формул (2.19), (2.20) випливає нерівність (2.18). Твердження доведено.

Зауважимо, що на відміну від формули (2.16), вираз у правій частині нерівності (2.18) явно залежить від параметра δ.

Безпосередньо з твердження 2.1 отримаємо наступний результат.

Наслідок 2.1. Для відновлення істинного розв'язку СР (2.7) з ймовірністю помилки не більше $\delta \in (0, 1/2)$ на другому етапі алгоритму, наведеного в п. 2.2, необхідно мати не менше ніж

$$m_{c,r'}(k, l') = \Delta_{c,r'}(k)^{-1}((1 - \delta)l'r' - h(\delta)) \ln 2 \tag{2.21}$$

рівнянь, де $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$, а $\Delta_{c,r'}(k)$ визначається за формулою (2.11).

3.4. Аналітичний вираз квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні потокові шифри

Надалі термін "кореляційна атака" означає одну з атак, описаних у підрозділі 2.2. Нагадаємо, що кожна така атака визначається дільником r' числа r та ненульовим елементом c поля F_{2^r} і полягає у складанні СР (2.7) та її подальшому розв'язанні за допомогою алгоритму з [7], який залежить від параметрів $k \geq 2$, що є степенем двійки, та $l' \in \overline{1,l}$, де $l = nr''$, $r'r'' = r$. При цьому інформаційна складність (другого етапу) атаки визначається за формулою (2.21), середня трудомісткість – за формулою (2.12), а обсяг матеріалу, потрібного для успішної реалізації атаки – за формулою (2.13).

Обидві формули містять вираз квадратичної евклідової незбалансованості, а саме, параметра $\Delta_{c,r'}(k)$, який на підставі рівностей (2.9), (2.11) має такий вигляд:

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\} - 1)^2, \qquad (2.22)$$

де $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$, а випадкова величина ξ_i визначається за формулою (2.5), $i \in \overline{1,k}$. Таким чином, для оцінювання ефективності кореляційних атак на SNOW 2.0-подібні потокові шифри або для обґрунтування стійкості цих шифрів

відносно зазначених атак треба вміти обчислювати (або оцінювати) значення параметра (2.22) безпосередньо за криптосхемою шифру.

Отримаємо вираз цього параметра в термінах коефіцієнтів Фур'є розподілу ймовірностей випадкових величин (2.5).

Нагадаємо, що перетворення Фур'є довільного розподілу $(p(z): z \in F_{2^m})$ на полі F_{2^m} визначається за формулою

$$\hat{p}(u) = \sum_{z \in F_{2^m}} p(z)(-1)^{\mathrm{Tr}_2^{2^m}(uz)},\ u \in F_{2^m},$$

де $\mathrm{Tr}_2^{2^m}(x) = x \oplus x^2 \oplus \cdots \oplus x^{2^{m-1}}$ – абсолютний слід довільного елемента $x \in F_{2^m}$. На підставі рівності Парсеваля (див., наприклад, [21], с. 27) справедлива формула

$$2^{-m} \sum_{z \in F_{2^m}} (2^m p(z) - 1)^2 = \sum_{u \in F_{2^m} \setminus \{0\}} |\hat{p}(u)|^2. \qquad (2.23)$$

Далі, згідно з теоремою про згортку ([21], с. 26), перетворення Фур'є розподілу суми незалежних випадкових величин дорівнює добутку перетворень Фур'є розподілів доданків. Звідси на підставі формул (2.22), (2.23) при $m = r'$, $p(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\}$, $z \in F_{2^{r'}}$, отримаємо рівність

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\varphi_c(u)|^{2k}, \qquad (2.24)$$

де

$$\varphi_c(u) = \sum_{z \in F_{2^{r'}}} \mathbf{P}\{\eta_i = z\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)},\ u \in F_{2^{r'}} \qquad (2.25)$$

є перетворенням Фур'є розподілу ймовірностей випадкової величини $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$.

Переконаємося у справедливості рівності

$$\varphi_c(u) = \hat{\pi}(uc),\ u \in F_{2^{r'}}, \tag{2.26}$$

де

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha x)},\ \alpha \in F_{2^r} \tag{2.27}$$

є перетворенням Фур'є розподілу ймовірностей випадкових величин (2.5).

Дійсно, використовуючи формулу (2.25), умову $u \in F_{2^{r'}}$ і транзитивність функції слід (див., наприклад, [14], теор. 2.26), отримаємо, що

$$\varphi_c(u) = \sum_{z \in F_{2^{r'}}} \mathbf{P}\{\mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i) = z\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)} = \sum_{z \in F_{2^{r'}}} \sum_{\substack{x \in F_{2^r}: \\ \mathrm{Tr}_{2^{r'}}^{2^r}(cx) = z}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)} =$$

$$= \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(u\mathrm{Tr}_{2^{r'}}^{2^r}(cx))} = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(\mathrm{Tr}_{2^{r'}}^{2^r}(ucx))} =$$

$$= \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(ucx)} = \hat{\pi}(uc).$$

Таким чином, справедлива рівність (2.26), з якої на підставі формули (2.24) випливає наступне твердження.

Твердження 2.2. Параметр (2.22) задовольняє рівності

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\hat{\pi}(uc)|^{2k}, \qquad (2.28)$$

де значення $\hat{\pi}(uc)$ визначається за формулою (2.26) при $\alpha = uc$.

Отримане твердження дозволяє оцінювати ефективність кореляційних атак на SNOW 2.0-подібні потокові шифри безпосередньо за коефіцієнтами Фур'є розподілу випадкових величин (2.5) і складає основу для наступних результатів, викладених у дисертації.

2.5. Порівняння ефективності кореляційних атак над скінченними полями різних порядків

Твердження 2.2 дозволяє отримати відповідь на запитання про те, наскільки більш ефективними (з погляду середньої трудомісткості та обсягу потрібного матеріалу) можуть бути кореляційні атаки над полями порядку $2^{r'}$, де $r' \geq 2$, в порівнянні з традиційними двійковими атаками на SNOW 2.0-подібні потокові шифри.

Справедливе таке твердження.

Твердження 2.3. Нехай $r'r'' = r$, де $r', r'' \in \mathbf{N}$, $c \in F_{2^r} \setminus \{0\}$, $k = 2^s$, де $s \in \mathbf{N}$, $l = nr''$ і $l' \in \overline{1,l}$. Позначимо α^* ненульовий елемент поля F_{2^r} такий, що

$$|\hat{\pi}(\alpha^*)| = \max_{\alpha \in F^r \setminus \{0\}} |\hat{\pi}(\alpha)|, \qquad (2.29)$$

де $\hat{\pi}(\alpha)$ визначається за формулою (2.26). Тоді для параметрів (2.12) та (2.13) справедливі такі нерівності:

$$T_{c,r'}(k,l') \geq (2^{r'}-1)^{-1} T_{\alpha^*,1}(k, r'l'), \tag{2.30}$$

$$N_{c,r'}(k,l') \geq (2^{r'}-1)^{-1} N_{\alpha^*,1}(k, r'l') \tag{2.31}$$

Таким чином, будь-яка кореляційна атака над полем $F_{2^{r'}}$ (з класу атак, що розглядається) є не більш ніж у $2^{r'}$ разів ефективніше (як за середньою трудомісткістю, так і за обсягом матеріалу) в порівнянні з найкращою кореляційною атакою над полем F_2.

Доведення. На підставі твердження 2.2 та формули (2.28) справедливі співвідношення

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\hat{\pi}(uc)|^{2k} \leq (2^{r'}-1)\,|\hat{\pi}(\alpha^*)|^{2k} = (2^{r'}-1)\,\Delta_{\alpha^*,1}(k).$$

Використовуючи формули (2.12), (2.21), отримаємо звідси, що

$$T_{c,r'}(k,l') = (\Delta_{c,r'}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2)^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} +$$

$$+ r'(\Delta_{c,r'}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2 + r'l'2^{r'l'}) + 2^{r'(l'+1)} \geq$$

$$\geq (2^{r'}-1)^{-\frac{1}{\theta}} (\Delta_{\alpha^*,1}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2)^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} +$$

$$+ r'(2^{r'}-1)^{-1}(2\Delta_{\alpha*,1}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2 + r'l'2^{r'l'}) + 2^{t'(l'+1)}.$$

Далі, вважаючи $l'' = r'l'$ та використовуючи рівності $r'l = r'nr'' = nr$, $r' \geq 1$, отримаємо такі співвідношення:

$$T_{c,r'}(k,l') \geq (2^{r'}-1)^{-1}(\Delta_{\alpha^*,1}(k)^{-1}((1-\delta)l'' - h(\delta))\ln 2)^{\frac{1}{\theta}} k 2^{\frac{nr-l''}{\theta}} +$$

$$+(2^{r'}-1)^{-1}(\Delta_{\alpha*,1}(k)^{-1}((1-\delta)l'' - h(\delta))\ln 2 + l''2^{l''}) + 2^{l''+1} = (2^{r'}-1)^{-1}T_{\alpha^*,1}(k,l'').$$

Отже, справедлива нерівність (2.30). Нерівність (2.31) доводиться аналогічно.

Твердження доведено.

Приклад 2.3. В [7] запропоновано кореляційну атаку на SNOW 2.0 над полем F_{2^8}, яка має середню трудомісткість $2^{164,15}$, потребує приблизно $2^{163,59}$ знаків гами і є суттєво швидше в порівнянні з раніше відомою двійковою атакою, трудомісткість якої складає $2^{212,38}$ [6].

Поряд з тим, на підставі твердження 2.3 існує двійкова кореляційна атака на SNOW 2.0, яка має середню трудомісткість не більше ніж $2^8 \cdot 2^{164,15} = 2^{172,15}$ та потребує не більше ніж $2^8 \cdot 2^{163,59} = 2^{171,59}$ знаків гами, причому параметри цієї атаки (вектор α^* та числа k і l') визначаються безпосередньо за параметрами вхідної атаки над полем F_{2^8} (див. формули (2.29), (2.30)).

Наведений приклад свідчить про те, що виграш у трудомісткості атаки з [7] в порівнянні з атакою в [6] досягається не стільки за рахунок застосування поля більшого порядку (F_{2^8} замість F_2), скільки в результаті вдалого вибору системи рівнянь зі спотвореними правими частинами для проведення атаки, а також застосування більш ефективного алгоритму розв'зання цієї системи рівнянь.

В цілому, згідно з твердженням 2.3, перехід від двійкових кореляційних атак до атак над полями порядку $2^{r'}$ може підвищити ефективність перших не більше ніж в $2^{r'}$ разів.

Висновки

1. У розділі викладено нові результати, які складають наукову основу розроблених дисертантом методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак, які будуються по аналогії з відомими атаками на SNOW 2.0 [3 – 7]. Кожна така атака визначається дільником r' степеня r поля, над яким задається ЛРЗ на рис. 2.1, та ненульовим елементом c цього поля і полягає у складанні СР (2.7) та її подальшому розв'язанні за допомогою алгоритму з [7], який залежить від параметрів $k \geq 2$, що є степенем двійки, та $l' \in \overline{1,l}$, де $l = nr''$, $r'r'' = r$. При цьому середня трудомісткість атаки визначається за формулою (2.12), а обсяг матеріалу, потрібного для реалізації атаки – за формулою (2.13).

2. Першим науковим результатом розділу є неасимптотична нижня оцінка інформаційної складності кореляційних атак, які базуються на розв'язані систем лінійних рівнянь зі спотвореними правими частинами над довільними скінченними полями характеристики 2 (див. твердження 2.1). Отримана оцінка має належне наукове обґрунтування. Вона уточнює раніше відому (евристичну) оцінку інформаційної складності [7] та є справедливою для будь-яких кореляційних атак на довільні потокові шифри незалежно від способу побудови або методу розв'язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

3. Другим науковим результатом розділу є аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень

у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні потокові шифри (див. твердження 2.2). Це співвідношення отримано вперше. Воно дозволяє звести задачу знаходження нижніх оцінок трудомісткості будь-якої кореляційної атаки з визначеного класу та обсягу матеріалу, потрібного для її успішної реалізації, до побудови верхніх меж максимуму модулів коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь системи (2.4), яка не залежить від конкретної атаки. Таким чином, ефективність кореляційних атак на SNOW 2.0-подібні потокові можна оцінити безпосередньо за коефіцієнтами Фур'є розподілу випадкових величин (2.5), що й складає основу для подальших наукових результатів дисертаційної роботи.

4. Будь-яка кореляційна атака над полем $F_{2^{r'}}$ (з класу атак, що розглядається) є не більш ніж у $2^{r'}$ разів ефективніше (як за середньою трудомісткістю, так і за обсягом матеріалу) в порівнянні з найкращою кореляційною атакою над полем F_2. Отже, перехід від двійкових кореляційних атак до атак над полями порядку $2^{r'}$ може підвищити ефективність перших не більше ніж в $2^{r'}$ разів.

5. Доведено, що існує двійкова кореляційна атака на шифр SNOW 2.0, яка має середню трудомісткість не більше ніж $2^{172,15}$, потребує не більше ніж $2^{171,59}$ знаків гами і, отже, є більш ніж у 2^{40} разів швидше в порівнянні з найкращою раніше відомою двійковою атакою на цей шифр [6].

Список використаних джерел у другому розділі

1. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography. SAC 2002. LNCS 2295. Springer-Verlag*. 2002. P. 47 – 61.

2. ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Psrt 4: Stream ciphers, 2011. 92 p.

3. Watanabe D., Biryukov A., de Cannière C. A distinguishing attack of SNOW 2.0 with linear masking method. *Selected Arreas in Cryptography SAC 2003. LNCS 3006. Springer-Verlag.* 2003. P. 222 – 233.

4. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption. FSE 2006. LNCS 4047. Springer-Verlag*. 2006. P. 144 – 162.

5. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology. ASIACRYPT 2005. LNCS 3788. Springer-Verlag*. 2005. P. 313 – 332.

6. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology. ASIACRYPT 2008. LNCS 5350. Springer-Verlag*. 2008. P. 524 – 538.

7. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive, Report 2016/311*. URL: http://eprint.iacr.org/2016/311 (дата звернення: 27.01.2020)

8. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018*, 24 – 27 May, 2018, Kyiv, Ukraine. P. 292 – 299.

9. *ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення*. 2019

10. Олексійчук А.М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами. *Захист інформації.* 2016. Т. 18. № 3. С. 261 – 268.

11. Daemen J., Rijmen D. AES proposal: Rijndael, URL: htpp://csrc.nist.gov/encription/aes/rijndael/ Rijndael.pdf (дата звернення: 27.01.2020)

12. Oliynykov R.V., Gorbenko I.D., Kazymyrov O.V. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/ 2015/650 (дата звернення: 27.01.2020)

13. Алексейчук А.Н., Ковальчук Л.В., Шевцов А.С., Яковлев С.В. О криптографических свойствах нового национального стандарта шифрования Украины. *Кибернетика и системный анализ*. 2016. Т. 52. № 3. С. 16 – 31.

14. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. / Пер. с англ. М.: Мир. 1988. – 818 с.

15. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM*. 2003. Vol. 50. № 3. P. 506 – 519.

16. Олексійчук А.М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. *Прикладная радиоэлектроника.* 2012. Т. 11. № 2. С. 3 – 11.

17. Bogos S., Tram′er F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis. *Cryptology ePrint Archive, Report 2015/049*. URL: http://eprint.iacr.org/2015/049 (дата звернення: 27.01.2020)

18. Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями, *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. Вип. 15. С. 150 – 155.

19. Wagner D. A generalized birthday problem. *Advances in Cryptology – CRYPTO'02, Proceedings. Springer Verlag*. 2002. P. 288 – 303.

20. Чечёта С.И. Введение в дискретную теорияю информации и кодирования: учебное издание. *М.: МЦНМО*. 2011. – 224 с.

21. Carlet C. Boolean functions for cryptography and error correcting codes. In Boolean Methods and Models. *Cambridge, U.K. Cambridge Univ. Press*. 2006.

РОЗДІЛ 3

МЕТОД ОБГРУНТУВАННЯ СТІЙКОСТІ ДВІЙКОВИХ SNOW 2.0-ПОДІБНИХ ШИФРІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК

Результати попереднього розділу дозволяють перейти безпосередньо до розробки методів обґрунтування стійкості SNOW 2.0-подібних шифрів відносно кореляційних атак, описаних в п. 2.2. При цьому відмінності у будові двійкових та модулярних шифрів відповідно потребують створення окремих методів оцінювання та обґрунтування їх стійкості.

Даний розділ присвячено викладенню методу обґрунтування стійкості двійкових ординарних SNOW 2.0-подібних шифрів, які мають більш просту будову в порівнянні з модулярними шифрами. Зазначений метод запропоновано вперше і базується на отриманих аналітичних нижніх оцінках трудомісткості та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на ординарні двійкові SNOW 2.0-подібні потокові шифри. Вирази отриманих оцінок залежать від параметрів, які традиційно використовуються для оцінювання стійкості блокових шифрів відносно лінійного криптоаналізу: максимальних елементів таблиць лінійних апроксимацій вузлів заміни та індексу галуження (branch number) лінійного перетворення у схемі алгоритму шифрування.

Застосування розробленого методу до двійкових версій шифрів SNOW 2.0 та “Струмок” показує, що будь-яка кореляційна атака на них (з визначеного класу) над полем порядку 256 має середню часову складність не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно,

$2^{249,38}$ знаків гами, що свідчить про практичну стійкість зазначених двійкових шифрів відносно відомих кореляційних атак.

3.1. Наукові основи методу, що пропонується

Розглянемо ординарний двійковий SNOW 2.0-подібний шифр, який отримується в результаті заміни операції $*$ у схемі на рис. 2.1 операцією $\oplus$. В цьому випадку випадкова величина (2.5) має вигляд $\xi_i = u_i \oplus \sigma(u_i)$, де u_i є випадковим вектором з рівномірним розподілом на множині V_r, $i = 0, 1, \ldots$.

Отримаємо аналітичний вираз та верхню оцінку параметра (2.22).

Надалі, згідно з означенням ординарного шифру в п. 2.1, вважатимемо, що $r = pt$, де $p, t \in \mathbf{N}$, $p, t \geq 2$, та існують базис B поля F_{2^r} над підполем F_{2^t}, підстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$ та оборотна $p \times p$-матриця D над полем F_{2^t} такі, що (при ототожненні елементів z та $\sigma(z)$ поля F_{2^r} з наборами їх координат в базисі B) виконується рівність (2.3).

Позначимо $\hat{\mathrm{B}}$ басиз, дуальний до базису B. Як і вище, ототожнюватимемо довільний елемент $z \in F_{2^r}$ з набором $(z_0, \ldots, z_{p-1})$ його координат в базисі B та позначатимемо цей набір тим самим символом: $z = (z_0, \ldots, z_{p-1})$. Символом $\hat{z} = (\hat{z}_0, \ldots, \hat{z}_{p-1})$ позначатимемо набір координат елемента $z \in F_{2^r}$ в базисі $\hat{\mathrm{B}}$. Надалі не зазначатимемо символ транспонування у формулах вигляду Dz^T, вважаючи (як звичайно), що вектор z є стовпцем, якщо він записаний справа від матриці D.

Для будь-якого $z = (z_0, \ldots, z_{p-1}) \in F_{2^t}{}^p$ покладемо

$$\mathrm{supp}(z) = \{ j \in \overline{0,\ p-1} : z_j \neq 0 \},\ wt(z) = |\,\mathrm{supp}(z)\,|.$$

Нагадаємо, (див., наприклад, [1]), що *індекс галуження* (branch number) матриці D^T визначається за формулою

$$B(D^T) = \min\{ wt(z) + wt(zD^T) : z \in F_{2^t}{}^p \setminus \{0\}, \tag{3.1}$$

а *елементи таблиці лінійних апроксимацій* підстановки s_j – за формулами [2]

$$l_{s_j}(a_j, b_j) = \left(2^{-t} \sum_{u_j \in F_{2^t}} (-1)^{\mathrm{Tr}_2^{2^t}(u_j a_j \oplus s_j(u_j) b_j)} \right)^2, a_j, b_j \in F_{2^t},\ j \in \overline{0,\ p-1}. \tag{3.2}$$

Зауважимо, що на підставі означення 2.30 в [3] вираз $\mathrm{Tr}_2^{2^t}(u_j a_j \oplus s_j(u_j) b_j)$ у формулі (3.2) можна замінити булевим скалярним добутком $u_j a_j \oplus s_j(u_j) b_j$, якщо ототожнити елементи $u_j, s_j(u_j)$ з векторами їх координат у певному базисі поля F_{2^t}, а елементи a_j, b_j – з векторами їх координат у відповідному дуальному базисі.

Доведемо твердження, яке верхню оцінку та, за певних умов, аналітичний вираз параметра (2.22) для ординарного двійкового SNOW 2.0-подібного шифру в термінах параметрів (3.1), (3.2).

Твердження 3.1. Справедлива нерівність

$$\Delta_{c,r'}(k) \le (2^{r'} - 1)\left(l_{\max}\right)^{\left\lceil \frac{B(D^T)}{2} \right\rceil k}, \tag{3.3}$$

де $l_{\max} = \max\{ l_{s_j}(a_j, b_j) : a_j, b_j \in F_{2^t} \setminus \{0\}, j \in \overline{0, p-1} \}$. Крім того, якщо r' є дільником числа t, то справедлива рівність

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} l_{s_0}(u\hat{c}_0, u\hat{c}'_0)^k \cdots l_{s_{p-1}}(u\hat{c}_{p-1}, u\hat{c}'_{p-1})^k , \qquad (3.4)$$

де $\hat{c} = (\hat{c}_0, \ldots, \hat{c}_{p-1})$ – вектор координат елемента $c \in F_{2^r}$ в базисі $\hat{\mathrm{B}}$, $(\hat{c}'_0, \ldots, \hat{c}'_{p-1}) = \hat{c}D^T$.

Доведення. Покажемо, що параметр (2.27) задовольняє такій рівності:

$$|\hat{\pi}(\alpha)|^2 = l_{s_0}(\hat{\alpha}_0, \hat{\alpha}'_0) \cdots l_{s_{p-1}}(\hat{\alpha}_{p-1}, \hat{\alpha}'_{p-1}), \qquad (3.5)$$

де $\hat{\alpha}' = (\hat{\alpha}'_0, \ldots, \hat{\alpha}'_{p-1}) = (\hat{\alpha}_0, \ldots, \hat{\alpha}_{p-1})D^T$.

Дійсно, в силу транзитивності функції сліду та дуальності базисів B і $\hat{\mathrm{B}}$ для будь-яких $x, \alpha \in F_{2^{pt}}$ справедливі рівності

$$\mathrm{Tr}_2^{2^{pt}}(x\alpha) = \mathrm{Tr}_2^{2^t}(\mathrm{Tr}_{2^t}^{2^{pt}}(x\alpha)) = \mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha}),$$

де $x \cdot \hat{\alpha}$ є скалярним добутком векторів $(x_0, \ldots, x_{p-1})$ та $(\hat{\alpha}_0, \ldots, \hat{\alpha}_{p-1})$ над полем F_{2^t}. Отже, на підставі формули (2.27) та рівності $\xi_i = u_i \oplus \sigma(u_i)$, $i = 0, 1, \ldots$, отримаємо такі співвідношення:

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^t}{}^p} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha})} =$$

$$= 2^{-r} \sum_{x \in F_{2^t}{}^p} \sum_{\substack{u \in F_{2^t}{}^p: \\ u \oplus \sigma(u) = x}} (-1)^{\mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha})} = 2^{-r} \sum_{u \in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}((u \oplus \sigma(u)) \cdot \hat{\alpha})} .$$

Використовуючи формулу (2.3), отримаємо звідси, що

$$\hat{\pi}(\alpha) = 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha}\oplus((s_0(u_0),\ldots,s_{p-1}(u_{p-1}))D)\cdot\hat{\alpha})} =$$

$$= 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha}\oplus(s_0(u_0),\ldots,s_{p-1}(u_{p-1}))\cdot(D\hat{\alpha}))} =$$

$$= 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha}\oplus(s_0(u_0),\ldots,s_{p-1}(u_{p-1}))\cdot\hat{\alpha})} =$$

$$= \prod_{j=0}^{p-1} \left(2^{-t} \sum_{u_j\in F_{2^t}} (-1)^{\mathrm{Tr}_2^{2^t}(u_j\hat{\alpha}_j\oplus s_j(u_j)\hat{\alpha}'_j)} \right).$$

Підносячи наведений вираз до квадрату, отримаємо формулу (3.5).

Підставляючи вираз у правій частині рівності (3.28) у формулу (3.20) на підставі співвідношення $F_{2^{r'}} \subseteq F_{2^t}$, отримаємо рівність (3.26).

Доведемо нерівність (3.3). Нехай α є ненульовим елементом поля F_{2^r} таким, що $|\hat{\pi}(\alpha)| = \max\limits_{\beta\in F^r\setminus\{0\}} |\hat{\pi}(\beta)|$. З твердження 2.1 випливає, що $\Delta_{c,r'}(k) \le (2^{r'}-1)\,|\hat{\pi}(\alpha)|^{2k}$. Звідси на підставі формул (3.2), (3.5) отримаємо, що $|\hat{\pi}(\alpha)| = 0$, якщо існує принаймні одне $j \in \overline{0,\, p-1}$ таке, що $\hat{\alpha}_j = 0$, $\hat{\alpha}'_j \neq 0$ або $\hat{\alpha}_j \neq 0$, $\hat{\alpha}'_j = 0$. Отже, за умови $|\hat{\pi}(\alpha)| \neq 0$ справедлива така рівність:

$$\mathrm{supp}(\hat{\alpha}) = \mathrm{supp}(\hat{\alpha}D^T).$$

Звідси на підставі формул (3.1) та (3.5) отримаємо, що

$$\Delta_{c,r'}(k) \le (2^{r'} - 1)\left(l_{\max}\right)^{\frac{wt(\hat{\alpha})}{2}k}, \; 2wt(\hat{\alpha}) \ge B(D^T),$$

Таким чином, нерівність (3.3.) доведено.

Припустимо зараз, що r' є дільником числа t. Підставляючи вираз у правій частині рівності (3.5) у формулу (2.28) на підставі співвідношення $F_{2^{r'}} \subseteq F_{2^t}$ отримаємо рівність (3.4). Це завершує доведення твердження.

Отримане твердження, поряд зі співвідношеннями (2.12), (2.13), (2.21) дозволяє оцінювати та обгрунтовувати стійкість ординарних двійкових SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полем порядку $2^{r'}$ безпосередньо за параметрами (3.1), (3.2) їх компонент. (Зауважимо, що ці параметри традиційно використовуються для оцінювання стійкості блокових шифрів відносно лінійного методу криптоаналізу). При цьому застосування замість параметра $\Delta_{c,r'}(k)$ його верхньої оцінки (3.3) у формулах (2.12), (2.13), (2.21) надає можливість отримувати нижні оцінки середньої трудомісткості та обсягу матеріалу, потрібного для проведення на шифр будь-якої з (наведених вище) кореляційних атак над полем порядку $2^{r'}$.

З твердження 3.1 випливає також, що для побудови кореляційних атак на ординарні двійкові SNOW 2.0-подібних шифри можна використовувати лише такі елементи $c \in F_{2^{pt}} \setminus \{0\}$, які задовольняють умові

$$\mathrm{supp}(\hat{c}) = \mathrm{supp}(\hat{c}D^T). \qquad (3.6).$$

У практично важливому випадку $B(D^T) = p+1$ (коли D є максимально дистанційно роздільною (МДР) матрицею; див., наприклад, [4], с. 312) згідно з теоремою 4 в [5] для кожного $l \geq \left\lceil \frac{B(D^T)}{2} \right\rceil$ існує точно

$$(2^t - 1)\binom{p}{l}\sum_{j=0}^{2l-(p+1)}(-1)^j\binom{2l-1}{j}2^{t(2l-(p+1+j))}$$

зазначених елементів c таких, що $wt(\hat{c}) = l$.

3.2. Формальний опис запропонованого методу

Метод призначений для отримання нижніх оцінок параметрів (2.12), (2.13), які визначають, відповідно, середню трудомісткість та обсяг матеріалу, потрібного для проведення на ординарний двійковий SNOW 2.0-подібний потоковий шифр будь-якої з кореляційних атак над полем порядку $2^{r'}$, описаних в п. 2.2.

Наукова новизна. Зазначений метод запропоновано вперше. *Сутність методу* базується на застосуванні аналітичного співвідношення (3.3), справедливість якого випливає з доведених вище тверджень 2.1, 2.2 і 3.1. Поряд з формулами (2.12), (2.13), (2.21), отримане співвідношення дозволяє оцінювати та обгрунтовувати стійкість ординарних двійкових SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полем порядку $2^{r'}$ безпосередньо за параметрами їх компонент, які визначаються за формулами (3.1) та (3.2).

Алгоритм реалізації методу наведено на рис. 3.1.

Приклади застосування методу. Розглянемо двійкову версію шифру SNOW 2.0, яка відрізняється від оригіналу [6] застосуванням операції $\overset{32}{+}$ замість $\oplus$ у схемі на рис. 3.1.

Параметри цього шифру мають такі значення: $t=8$, $p=4$, $n=16$. При цьому підстановка σ має вигляд (2.3), де підстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$, та матриця D задаються так само, як у перетворенні шифру Rijndaep (див. приклад 2.1). Зокрема, відомо, що $l_{\max} = 2^{-6}$, $B(D^T) = p+1 = 5$ [12].

Використовуючи алгоритм 3.1, отримаємо нижні межі параметрів, що визначають ефективність кореляційних атак над полем $F_{2^t} = F_{256}$ на двійкову версію шифру SNOW 2.0 (табл. 3.1).

Таблиця 3.1

Результати виконання алгоритму 3.1 для двійкової версії шифру SNOW 2.0 ($r' = t$, $\delta = 0{,}01$)

k	l^*	$\log T_{r'}(k, l^*)$	$\log N_{r'}(k, l^*)$
2	22	187,84	186,97
4	17	151,24	151,19
8	12	146,20	142,77
16	1	292,45	161,50

Як ще один практично важливий приклад, розглянемо шифр “Струмок” [9], де використовуються такі параметри: $t=8$, $p=8$, $n=16$. При цьому підстановка σ має вигляд (2.3), де вузли заміни та матриця D задаються так само, як у блоковому шифрі “Калина” (див. приклад 2.2). Зокрема, відомо, що $l_{\max} = 9 \cdot 2^{-8}$, $B(D^T) = p+1 = 9$ [10]. Використовуючи алгоритм 3.1, отримаємо

значення параметрів, що визначають ефективність кореляційних атак над полем $F_{2^t} = F_{256}$ на двійкову версію шифру “Струмок” (табл. 3.2).

Алгоритм 3.1

Вхідні дані:

– натуральні числа n, p, t;

– підстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$;

– оборотна $p \times p$-матриця D над полем F_{2^t}.

– число $k \geq 2$, що є степенем двійки;

– дільник r' числа r;

– допустима верхня межа δ ймовірності помилки атаки.

1. Обчислити значення $\Delta_{r'}(k) = (2^{r'} - 1)\left(l_{\max}\right)^{\left\lceil \frac{B(D^T)}{2} \right\rceil_k}$, використовуючи формули (3.1) ,(3.2).

2. Покласти $r'' = pt(r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.

3. Для кожного $l' = 1, 2, ..., l-1$ обчислити

$$m_{r'}(k) = (\Delta_{r'}(k))^{-1}((1-\delta)l'r' - h(\delta))\ln 2,$$

$$T_{r'}(k, l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r'l'2^{r'l'}) + 2^{r'(l'+1)}.$$

4. Обрати $l^* \in \overline{1, l-1}$ таке, що $T_{r'}(k, l^*) = \min\{T_{r'}(k, l') : l' \in \overline{1, l-1}\}$.

Результат:

– число l^* фрагментів (довжини r' бітів кожний) початкового стану генератора, які відновлюються за допомогою атаки;

– середня часова складність атаки $T_{r'}(k, l^*)$;

– обсяг матеріалу

$$N_{r'}(k, l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}},$$

потрібного для успішної реалізації атаки.

Рис. 3.1. Алгоритм реалізації методу обгрунтування стійкості ординарних двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак

Таблиця 3.2

Результати виконання алгоритму 3.1 для двійкової версії шифру "Струмок" ($r' = t$, $\delta = 0{,}01$)

k	l^*	$\log T_{r'}(k, l^*)$	$\log N_{r'}(k, l^*)$
2	44	363,91	361,62
4	34	285,42	285,06
8	29	249,40	249,38
16	1	384,88	283,58

Подальше збільшення значення k в алгоритмі 3.1 приводить до збільшення значень параметрів $T_{r'}(k, l^*)$, $N_{r'}(k, l^*)$ в табл. 3.2. Отже, будь-яка з (розглянутих вище) кореляційних атак над полем порядку 256 на двійкову версію шифру "Струмок" має середню часову складність не менше ніж $2^{249,40}$ та потребує не менше ніж $2^{249,38}$ знаків гами.

В цілому, отримані результати свідчать про практичну стійкість двійкових версій шифрів SNOW 2.0 та "Струмок" до розглянутих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

3.3. Експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак

Розроблений метод дозволяє отримати відповідь на запитання про те, наскільки великою є частка вузлів заміни (серед усіх підстановок на множині V_t), які при фіксованих значеннях решти параметрів ординарного двійкового

SNOW 2.0-подібного шифру забезпечують його стійкість відносно розглянутих кореляційних атак на рівні заданого порогу (наприклад, не меншу або порівняну зі стійкістю двійкової версії шифру “Струмок”). Відповідь на це запитання має практично важливе значення в тому випадку, коли підстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$ використовуються як додаткові (довгострокові) ключові параметри алгоритму потокового шифрування. Якщо зазначені підстановки генеруються незалежно випадково та рівноймовірно, то середній час формування однієї з них, що задовольняє певному критерію, є обернено пропорційним частці підстановок, які задовольняють цьому критерію, у їх загальній сукупності. Тому відповідь на поставлене запитання дозволяє оцінити середній час, який потрібно витратити на формування довгострокових ключів ординарного двійкового SNOW 2.0-подібного шифру (принаймні, виходячи з критерію його стійкості відносно кореляційних атак).

На підставі тверджень 2.1, 2.2 і 3.1 поставлене запитання зводиться до наступного.

Для будь-якої підстановки s на множині V_t позначимо $l_{\max}(s)$ максимум значень вигляду (3.1) за всіма ненульовими елементами $a_j, b_j \in F_{2^t}$. Для кожного $x \in (0,1)$ позначимо $F(x)$ відносне число (частку) тих підстановок s (серед усіх можливих на множині V_t), для яких $l_{\max}(s) < x$. Треба побудувати статистичну оцінку параметра $F(x)$ із заданими точністю ε та достовірністю $1-\delta$, де $\varepsilon, \delta \in (0,1)$.

Для розв’язання цієї задачі скористаємося алгоритмом 3.2, який базується на методі Монте-Карло, а також на відомому алгоритмі швидкого перетворення Адамара (див., наприклад, [11]).

На підставі нерівності Чернова (див., наприклад, [12]), значення $F(x)$, яке треба оцінити, знаходиться в інтервалі $(F_N(x)-\varepsilon, F_N(x)+\varepsilon)$ з ймовірністю не менше ніж $1-\delta$, де $F_N(x)$ є результатом виконання алгоритму 3.2.

В табл. 3.3 наведено результати, отримані на перших трьох кроках алгоритму 3.2 при $t=8$, $\varepsilon=0{,}037$, $\delta=0{,}01$.

Таблиця 3.3

Значення параметрів, що визначають стійкість ординарних двійкових SNOW 2.0-подібних шифрів з випадково згенерованими вузлами заміни

$N(l_{\max})$	$l_{\max}$	k	$l*$	$\log T_{r'}(k,l*)$	$\log N_{r'}(k,l*)$
761	0,070556640625	2	43	360,62	360,58
		4	33	281,03	281,01
		8	28	241,33	241,32
		16	1	304,48	267,50
639	0,0791015625	2	43	359,83	359,75
		4	33	279,96	279,91
		8	28	239,73	239,67
		16	1	291,29	264,86
275	0,088134765625	2	43	359,10	358,97
		4	33	278,98	278,879
		8	28	238,27	238,11
		16	1	278,81	262,36
194	0,0625	2	43	361,48	361,45
		4	33	282,19	282,171
		8	28	243,08	243,07
		16	1	318,48	270,30
92	0,09765625	2	43	358,44	358,23

		4	33	278,09	277,8
		8	28	237,04	236,63
		16	1	266, 98	259,99
27	0,107666015625	2	43	357,86	357,53
		4	33	277,32	276,94
		8	28	236,17	235,22
		16	2	257,54	256,34
9	0,1181640625	2	43	357,35	356,86
		4	33	276,69	276,05
		8	28	235,55	232,88
		16	8	248,14	244,99
3	0,054931640625	2	43	362,40	362,38
		4	33	283,42	283,42
		8	29	244,00	242,954
		16	1	333,37	273,27

У другій колонці табл. 3.3 показані точні значення $l_{\max}(s_i)$, отримані для $N = \lceil 1/2 \cdot \varepsilon^{-2} \ln(2\delta^{-1}) \rceil = 2000$ випадкових рівноймовірних підстановок $s_i : V_t \to V_t$, а в першій колонці – кількість $N(l_{\max})$ підстановок із заданим значенням параметра $l_{\max}$. Результати в останніх трьох колонках табл. 3.3 отримано за допомогою алгоритму 3.1 при тих самих вхідних даних, що й для двійкової версії шифру “Струмок”: $t = 8$, $p = 8$, $n = 16$, $B(D^T) = p + 1 = 9$, $r' = t$, $\delta = 0{,}01$. Обчислення проведено в macOS Mojave 10.14, 2.2 GHz Intel Core i7, 16 GB 2400 MHz DDR4, Intel UHD Graphics 630 1536 MB).

Алгоритм 3.2

Вхідні дані:

– натуральне число t;

– підстановка $s: F_{2^t} \to F_{2^t}$;

– числа $\varepsilon, \delta \in (0,1)$;

– число $x \in (0,1)$.

1. Обчислити $N = \left\lceil 1/2 \cdot \varepsilon^{-2} \ln(2\delta^{-1}) \right\rceil$.

2. Згенерувати незалежні випадкові рівноймовірні підстановки $s_1, ..., s_N$.

3. Для кожного $i \in \overline{1,N}$ обчислити значення $l_{\max}(s_i)$, використовуючи наступну процедуру.

3.1. Для кожного $b \in V_t \setminus \{0\}$:

– обчислити значення функції $h_b(u) = (-1)^{s_i(u)b}$, $u \in V_t$;

– обчислити $l_{s_i}(a,b) = \left(2^{-t} \sum_{u \in V_t} (-1)^{ua} h_b(u) \right)^2$, $a \in V_t$ за допомогою алгоритму швидкого перетворення Адамара;

– покласти $l_{\max}(b) = \max\{ l_{s_i}(a,b) : a \in V_t \setminus \{0\} \}$.

3.2. Покласти $l_{\max}(s_i) = \max\{ l_{s_i}(b) : b \in V_t \setminus \{0\} \}$.

4. Підрахувати число $F_N(x)$ таких значень $i \in \overline{1,N}$, для яких $l_{\max}(s_i) < x$.

Результат: значення $F_N(x)$.

Рис. 3.2. Алгоритм статистичного оцінювання розподілу параметра $l_{\max}(s)$ як функції випадкової рівноймовірної підстановки s

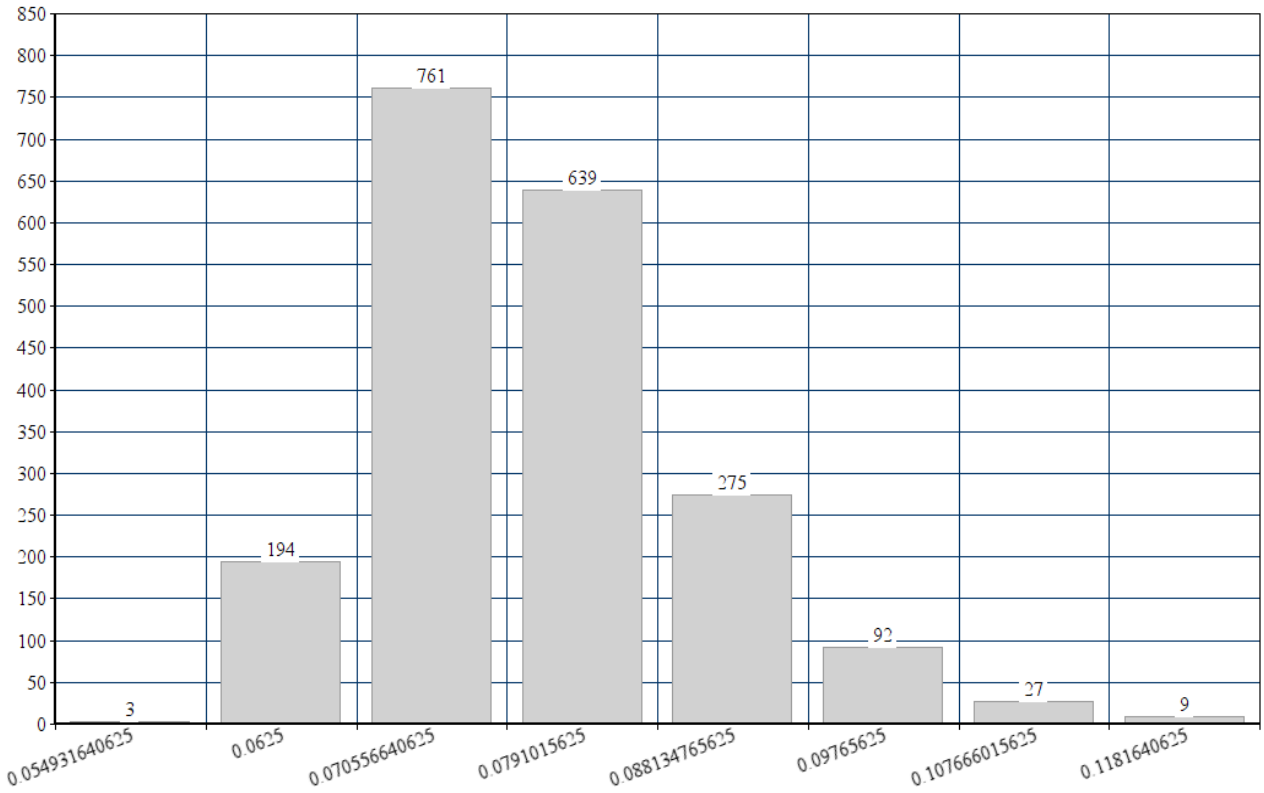

Рисунок 3.3. Гістограма, побудована за виборкою з 2000 випадкових рівноймовірних підстановок

На рис. 3.3 показано гістограму емпіричного розподілу ймовірностей випадкової величини $l_{\max}(s)$, де s є випадковою рівноймовірною підстановкою на множині V_t при $t = 8$.

Як видно з рис. 3.3 і табл. 3.3, при $x = 0{,}071$ умова $l_{\max}(s) < x$ виконується для $761 + 194 + 3 = 958$ з $N = 2000$ випадково згенерованих підстановок s. При цьому середня трудомісткість кореляційної атаки на SNOW 2.0-подібний шифр з такими підстановками (що використовується в ролі вузлів заміни

$s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$) є не менше ніж $2^{241,33}$. Отже, $F_N(x) = \dfrac{958}{2000} = 0{,}479$ і з достовірністю принаймні $1-\delta$ (тобто 99 %) відносне число всіх підстановок, які забезпечують стійкість шифру до кореляційних атак на рівні не менше ніж $2^{241,33}$, знаходиться в межах від $0{,}479-\varepsilon$ до $0{,}479+\varepsilon$. Іншими словами, майже кожна друга випадково згенерована підстановка забезпечує стійкість відповідного SNOW 2.0-подібного шифру на рівні $2^{241,33}$.

При $x = 0{,}119$ маємо $F_N(x) = 1$; при цьому, оскільки найменше значення $\log T_{r'}(k, l^*)$ у четвертій колонці табл. 3.3 дорівнює 235,55, то середня трудомісткість атаки на шифр є не менше ніж $2^{235,55}$. Таким чином, з достовірністю принаймні 99 % частка підстановок, які забезпечують зазначену стійкість SNOW 2.0-подібних шифрів, складає не менше ніж $1-\varepsilon$.

В цілому, отримані результати показують, що при використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$, в ролі довгострокових ключових параметрів ординарних двійкових SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість шифрів відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу.

Поряд з тим, є й напевно "слабкі" (наприклад, афінні) підстановки, застосовувати які в ролі вузлів заміни SNOW 2.0-подібних шифрів є неприпустимим. Проте, як видно з табл. 3.3, частка таких "слабких" підстановок серед усіх можливих є практично непомітною.

Висновки

1. Основним науковим результатом розділу є метод обґрунтування стійкості ординарних двійкових SNOW 2.0-подібних шифрів відносно

кореляційних атак, описаних в п. 2.2. Зазначений метод запропоновано вперше і базується на застосуванні аналітичного співвідношення (3.3), справедливість якого випливає з доведених вище тверджень 2.1, 2.2 і 3.1. Поряд з формулами (2.12), (2.13), (2.21), отримане співвідношення дозволяє оцінювати та обґрунтовувати стійкість ординарних двійкових SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полем порядку $2^{r'}$ безпосередньо за параметрами їх компонент, які визначаються за формулами (3.1) та (3.2).

2. Стійкість ординарних двійкових SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полем порядку $2^{r'}$ залежить безпосередньо від максимальних елементів таблиць лінійних апроксимацій вузлів заміни та індексу галуження (branch number) лінійного перетворення у схемах алгоритмів потокового шифрування. Поряд з тим, зазначені параметри традиційно використовуються для оцінювання стійкості блокових шифрів відносно лінійного методу криптоаналізу.

3. Застосування розробленого методу до двійкових версій шифрів SNOW 2.0 та "Струмок" показує, що будь-яка кореляційна атака на них (з визначеного класу) над полем порядку 256 має середню трудомісткість не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно, $2^{249,38}$ знаків гами, що свідчить про практичну стійкість зазначених двійкових шифрів відносно відомих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

4. При використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, в ролі довгострокових ключових параметрів ординарних двійкових SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу. Зокрема, з достовірністю принаймні 99 % відносне число всіх підстановок, які

забезпечують стійкість шифру відносно кореляційних атак на рівні не менше ніж $2^{241,33}$, знаходиться в межах від $0,442$ до $0,516$. При цьому з достовірністю принаймні 99 % частка тих підстановок, які забезпечують стійкість на рівні не менше ніж $2^{235,55}$, складає щонайменше 0,963.

Список використаних джерел у третьому розділі

1. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. *Doctoral Dissertation*. 1995.

2. Chabaud F. *Vaudenay S.* Links between differential and linear cryptanalysis. *Advances in Cryptology. EUROCRYPT'94, Proceedings. Springer Verlag*. 1995. P. 356 – 365.

3. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. / Пер. с англ. *М.: Мир*. 1988. – 818 с.

4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. *М.: Связь*. 1979. 743 с.

5. Глухов М.М. О рассеивающих линейных преобразованиях для блочных шифрсистем. *Математические вопросы криптографии.* 2011. Т. 2. № 2. С. 5 – 40.

6. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography. SAC 2002. LNCS 2295. Springer-Verlag*. P. 47 – 61.

7. Daemen J., Rijmen D. AES proposal: Rijndael, URL: htpp://csrc.nist.gov/encription/aes/rijndael/Rijndael.pdf (дата звернення: 27.01.2020)

8. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive, Report 2016/311*. URL: http://eprint.iacr.org/2016/311 (дата звернення: 27.01.2020)

9. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018, 24 – 27 May, 2018, Kyiv, Ukraine*. P. 292 – 299.

10. Алексейчук А.Н., Ковальчук Л.В., Шевцов А.С., Яковлев С.В. О криптографических свойствах нового национального стандарта шифрования Украины. *Кибернетика и системный анализ*. 2016. Т. 52. № 3. С. 16 – 31.

11. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. *М.: МЦНМО*. 2004. – 470 с.

12. Hoeffding W. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc.* 1963. Vol. 58. № 301. P. 13 – 30.

РОЗДІЛ 4

МЕТОД ОБГРУНТУВАННЯ СТІЙКОСТІ МОДУЛЯРНИХ NOW 2.0-ПОДІБНИХ ШИФРІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК

Вище зазначено, що розповсюдження результатів розділу 3 на модулярні SNOW 2.0-подібні шифри наштовхується на труднощі, пов'язані із застосуванням у схемах таких шифрів операції додавання двійкових цілих чисел за модулем степеня двійки. Відомі методи, розвинуті для подолання цих труднощів [1 – 3] передбачають обчислення розподілів ймовірностей спотворень у правих частинах СР, які використовуються для побудови кореляційних атак, і виявляються незастосовними, коли порядок поля, над яким визначено шифр, складає 2^{64} або більше (наприклад, для шифру "Струмок"). Крім того, зазначені методи орієнтовані на побудову конкретних атак, а не на обґрунтування стійкості SNOW 2.0-подібних шифрів, тому їх застосування з метою обґрунтування стійкості, навіть у випадку шифру SNOW 2.0, призводить до великого обсягу обчислень.

З метою подолання цих недоліків в даному розділі пропонується теоретико-автоматний підхід до побудови верхніх оцінок незбалансованості дискретних відображень, які реалізуються послідовностями скінченних автоматів. Джерелом цього підходу є робота [4], де отримано матричне представлення для числа прообразів вихідної послідовності скінченного автомата; проте, у випадку, що розглядається нижче, йдеться не про розподіл числа прообразів, а про коефіцієнти Фур'є цього розподілу.

Основним науковим результатом розділу є метод обґрунтування стійкості модулярних SNOW 2.0-побдібних потокових шифрів відносно кореляційних атак, описаних в розділі 2. Метод базується на отриманих дисертантом

твердженнях 4.1, 4.2 і 4.3, перше з яких узагальнює низку окремих результатів про матричні (або лінійні) представлення незбалансованості відображень, які реалізуються автоматами спеціального вигляду [1, 5], а друге і третє надають верхні оцінки незбалансованості, які можуть бути використані, зокрема, для обґрунтування стійкості ординарних модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак.

За допомогою твердження 4.4 отримано нижні межі трудомісткості та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на ординарні модулярні SNOW 2.0-подібні шифри. Вирази отриманих меж залежать від певних параметрів вузлів заміни, які можна розглядати як модифіковані елементи їх таблиць лінійних апроксимацій, а також від індексу галуження лінійного перетворення у схемі алгоритму шифрування. Застосування отриманих меж до шифрів SNOW 2.0 та "Струмок" приводить до результатів, які співпадають з результатами, отриманими для їх двійкових версій: будь-яка кореляційна атака на зазначені шифри (з визначеного класу атак) над полем порядку 256 має середню часову складність не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно, $2^{249,38}$ знаків гами. Це свідчить про практичну стійкість шифрів SNOW 2.0 та "Струмок" відносно відомих кореляційних атак.

4.1. Наукові основи методу, що пропонується

4.1.1. Верхні оцінки незбалансованості відображень, що реалізуються послідовностями скінченних автоматів.

Нехай U, X – скінченні множини, $h_i : U \times X \to U$, $f_i : U \times X \to V_t$ – відображення, $i = 0, 1, \ldots$. Для будь-якого натурального n задано відображення $H_n : U \times X^n \to U$ і $F_n : U \times X^n \to V_t^n$, вважаючи

$$H_n(u_0, x_0, ..., x_{n-1}) = u_n,$$

$$F_n(u_0, x_0, ..., x_{n-1}) = y_0, y_1, ..., y_{n-1}, \qquad (4.1)$$

де елементи $u_1, u_2, ...,\ y_0, y_1, ...$ обчислюються за допомогою рекурентних співвідношень $u_{i+1} = h_i(u_i, x_i),\ y_i = f_i(u_i, x_i),\ i = 0, 1, ...$

Якщо $h_i = h,\ f_i = f$ для кожного $i = 0, 1, ...,$ то $F_n(u_0, x_0, ..., x_{n-1})$ є вихідною послідовністю автомата (X, U, V_t, h, f) (з вхідним алфавітом X, множиною станів U та вихідним алфавітом V_t), яка виробляється за його початковим станом u_0 та вхідною послідовністю $x_0, ..., x_{n-1}$, а $H_n(u_0, x_0, ..., x_{n-1})$ є станом цього автомата в n-му такті.

За означенням відображення $F : X^n \to V_t^{\,n}$ *реалізується послідовністю автоматів* $(X, U, V_t, h_i, f_i),\ i = \overline{0, n-1}$, якщо існує елемент $u_0 \in U$ такий, що $F(x_0, ..., x_{n-1}) = F_n(u_0, x_0, ..., x_{n-1})$ для кожного $(x_0, ..., x_{n-1}) \in X^n$.

Нехай $\alpha = (\alpha_0, \alpha_1, ...)$ є послідовністю двійкових векторів, $\alpha_i \in V_t$, $i = 0, 1, ...$ Для будь-якого натурального n позначимо $\alpha^{(n)} = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ та задамо функцію $F_n\alpha^{(n)}$, значення якої в точці $(u_0, x_0, ..., x_{n-1})$ дорівнює булевому скалярному добутку векторів $F_n(u_0, x_0, ..., x_{n-1})$ та $\alpha^{(n)}$. *Незбалансованість цієї функції при фіксованому значенні* $u_0 \in U$ визначається за формулою

$$l_\alpha^{(n)}(u_0) = \frac{1}{|X|^n} \left| \sum_{(x_0, ..., x_{n-1}) \in X^n} (-1)^{F_n(u_0, x_0, ..., x_{n-1})\alpha^{(n)}} \right|. \qquad (4.2)$$

Отримаємо матричне представлення та верхні оцінки параметра (4.2). Для будь-яких $u,u' \in U$ позначимо

$$l_{\alpha}^{(n)}(u,u') = \frac{1}{|X|^n} \sum_{\substack{(x_0,\dots,x_{n-1})\in X^n:\\ H_n(u,x_0,\dots,x_{n-1})=u'}} (-1)^{F_n(u,x_0,\dots,x_{n-1})\alpha^{(n)}} . \qquad (4.3)$$

Занумеруємо довільним чином елементи множини U, вважаючи $U = \{u_0, u_1, \dots, u_{M-1}\}$, де $M = |U|$, та задамо $M \times M$-матриці $A_{\alpha_i}^{(i)}$ з елементами

$$A_{\alpha_i}^{(i)}(u,u') = \frac{1}{|X|} \sum_{x\in X:\, h_i(u,x)=u'} (-1)^{f_i(u,x)\alpha_i} , \; u,u' \in U , \qquad (4.4)$$

де $f_i(u,x)\alpha_i$ позначає булевий скалярний добуток зазначених двійкових векторів довжини t, $i = 0, 1, \dots$.

Твердження 4.1. Для будь-якого натурального n справедлива рівність

$$l_{\alpha}^{(n)}(u,u') = (A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)})(u,u') , \; u,u' \in U ; \qquad (4.5)$$

іншими словами, параметр (4.3) співпадає з (u,u')-м елементом добутку матриць (4.4) за всіма $i \in \overline{0,n-1}$. Крім того, параметр (4.2) задовольняє такій рівності:

$$l_{\alpha}^{(n)}(u_0) = \left| \mathbf{e}\, A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)}\, \mathbf{1} \right| , \qquad (4.6)$$

де $\mathbf{e} = (1, 0, \dots, 0)$, $\mathbf{1} = (1, 1, \dots, 1)^T$.

Доведення. Формула (4.5) доводиться за допомогою індукції по n. При $n=1$ вона випливає безпосередньо з наведених означень. При $n \geq 2$ достатньо переконатися у справедливості такої рівності:

$$l_{\alpha}^{(n)}(u,u') = \sum_{u'' \in U} l_{\alpha}^{(n-1)}(u,u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'',u'),\ u,u' \in U. \qquad (4.7)$$

Дійсно, на підставі формул (4.3), (4.4) та означень відображень H_n, F_n мають місце такі співвідношення:

$$\sum_{u'' \in U} l_{\alpha}^{(n-1)}(u,u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'',u') =$$

$$= \frac{1}{|X|^n} \sum_{u'' \in U} \sum_{\substack{(x_0,\ldots,x_{n-2}) \in X^{n-1}: \\ H_{n-1}(u,x_0,\ldots,x_{n-2})=u''}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)}} \sum_{\substack{x_{n-1} \in X: \\ h_{n-1}(u'',x_{n-1})=u'}} (-1)^{f_{n-1}(u'',x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{(x_0,\ldots,x_{n-2}) \in X^{n-1}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)}} \times$$

$$\times \sum_{\substack{x_{n-1} \in X: \\ h_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1})=u'}} (-1)^{f_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{\substack{(x_0,\ldots,x_{n-2}) \in X^{n-1},\ x_{n-1} \in X: \\ H_n(u,x_0,\ldots,x_{n-1})=u'}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)} \oplus f_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{\substack{(x_0,\dots,x_{n-1})\in X^n: \\ H_n(u,x_0,\dots,x_{n-1})=u'}} (-1)^{F_n(u,x_0,\dots,x_{n-1})\alpha^{(n)}} = l_\alpha^{(n)}(u,u').$$

Отже, справедлива рівність (4.7), що і треба було довести.

Нарешті, справедливість рівності (4.6) випливає з формули (4.5) та наступної рівності: $l_\alpha^{(n)}(u_0) = \left| \sum_{u'\in U} l_\alpha^{(n)}(u_0, u') \right|$.

Таким чином, твердження повністю доведено.

Зауважимо, що твердження 4.1 узагальнює низку окремих результатів про матричні (або лінійні) представлення параметрів вигляду (4.2) для відображень, які реалізуються скінченними автоматами спеціального вигляду [1, 5]. Зазначене твердження дозволяє отримати верхні оцінки цього параметра, які можуть бути використані, зокрема, для обґрунтування стійкості ординарних модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак.

Введемо декілька додаткових позначень. Для будь-якого вектора $x = (x_1,\dots,x_n)$ з дійсними координатами позначимо

$$\| x \|_1 = |x_1| + \dots + |x_n|, \quad \| x \|_\infty = \max\{|x_i| : i \in \overline{1,n}\}.$$

Задамо звичайним чином sup-норму дійсної $n\times n$-матриці A, вважаючи $\| A \|_\infty = \sup\{\| Ax \|_\infty : \| x \|_\infty = 1\}$, де супремум береться за всіма дійсними векторами $x = (x_1,\dots,x_n)^T$ такими, що $\| x \|_\infty = 1$. Неважко переконатися в тому, що

$$\| A \|_\infty = \max\{\| A_1 \|_1, \| A_2 \|_1, \dots, \| A_n \|_1\}, \tag{4.8}$$

де $A_1, A_2, \ldots, A_n$ – рядки матриці A. Крім того, для будь-яких дійсних $n \times n$-матриць A та B справедлива нерівність

$$\| AB \|_\infty \le \| A \|_\infty \| B \|_\infty . \tag{4.9}$$

Твердження 4.2. Параметр (4.2) задовольняє нерівності

$$l_\alpha^{(n)}(u_0) \le \left\| A_{\alpha_0}^{(0)} \right\|_\infty \left\| A_{\alpha_1}^{(1)} \right\|_\infty \cdots \left\| A_{\alpha_{n-2}}^{(n-2)} \right\|_\infty \left\| A_{\alpha_{n-1}}^{(n-1)} \mathbf{1} \right\|_\infty , \tag{4.10}$$

де

$$\left\| A_{\alpha_i}^{(i)} \right\|_\infty = \max_{u \in U} \left\{ \frac{1}{|X|} \sum_{u' \in U} \left| \sum_{x \in X:\, h_i(u,x) = u'} (-1)^{f_i(u,x)\alpha_i} \right| \right\}, \; i \in \overline{0, n-2},$$

$$\left\| A_{\alpha_{n-1}}^{(n-1)} \mathbf{1} \right\|_\infty = \max_{u \in U} \left\{ \frac{1}{|X|} \left| \sum_{x \in X} (-1)^{f_{n-1}(u,x)\alpha_{n-1}} \right| \right\}.$$

Крім того, справедлива така нерівність:

$$\max_{(\alpha_0,\ldots,\alpha_{n-1}) \ne (0,\ldots,0)} \{ l_\alpha^{(n)}(u_0) \} \le \max_{i \in \overline{0,n-1}} \; \max_{\alpha_i \ne 0} \left\{ \left\| A_{\alpha_i}^{(i)} \mathbf{1} \right\|_\infty \right\}. \tag{4.11}$$

Доведення. Нерівність (4.10) випливає безпосередньо з рівності (4.6) та формул (4.8), (4.9).

Доведемо нерівність (4.11). Позначимо i найбільше число від 0 до $n-1$ таке, що $\alpha_i \ne 0$. Оскільки $\alpha_{i+1} = \ldots = \alpha_{n-1} = 0$, то на підставі формули (4.4)

$A^{(i+1)}_{\alpha_{i+1}} \cdots A^{(n-1)}_{\alpha_{n-1}} \mathbf{1} = \mathbf{1}$, звідки в силу формули (4.6) випливає, що $l^{(n)}_{\alpha}(u_0) = \left| \mathbf{e}\, A^{(0)}_{\alpha_0} A^{(1)}_{\alpha_1} \cdots A^{(i)}_{\alpha_i}\, \mathbf{1} \right|$. Отже,

$$l^{(n)}_{\alpha}(u_0) \le \left\| A^{(0)}_{\alpha_0} \right\|_{\infty} \cdots \left\| A^{(i-1)}_{\alpha_{i-1}} \right\|_{\infty} \left\| A^{(i)}_{\alpha_i} \mathbf{1} \right\|_{\infty} \le \left\| A^{(i)}_{\alpha_i} \mathbf{1} \right\|_{\infty},$$

що і треба було довести.

Твердження доведено.

Як приклад застосування тверджень 4.1 і 4.2, розглянемо довільний набір підстановок $s = (s_0, \ldots, s_{p-1})$ та вектори $\alpha = (\alpha_0, \ldots, \alpha_{p-1})$, $\beta = (\beta_0, \ldots, \beta_{p-1})$, де $s_i : V_t \to V_t$, $\alpha_i, \beta_i \in V_t$, $i \in \overline{0, p-1}$, і отримаємо верхню оцінку параметра

$$l_{\alpha,\beta}(s) = 2^{-2tp} \left| \sum_{x,y \in {V_t}^p} (-1)^{\overset{pt}{((x+y) \oplus x)\alpha \oplus s(y)\beta}} \right|, \tag{4.12}$$

де $x = (x_0, \ldots, x_{p-1})$, $y = (y_0, \ldots, y_{p-1})$, $s(y) = (s_0(y_0), \ldots, s_{p-1}(y_{p-1}))$, $x_i, y_i \in V_t$, $i \in \overline{0, p-1}$, а $\overset{pt}{x+y}$ позначає суму за модулем 2^{pt} двійкових цілих чисел, що відповідають векторам x, y (тут і далі будь-який вектор $x = (x_0, \ldots, x_{p-1}) \in {V_t}^p$ ототожнюється з цілим числом, наймолодший розряд якого співпадає з найлівішою координатою вектора x_0).

Для будь-яких $a, b \in V_t$, $i \in \overline{0, p-1}$ задамо 2×2-матрицю $A^{(i)}_{a,b}$ з елементами

$$A^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{\substack{x_i, y_i \in V_t: \\ \mathrm{msb}(\overset{t}{x_i} + \overset{t}{y_i} + u) = u'}} (-1)^{(\overset{t}{x_i} + \overset{t}{y_i} + u)a \oplus x_i a \oplus s_i(y_i) b}, \; u, u' \in \{0,1\}, \tag{4.13}$$

де $\mathrm{msb}(x_i + y_i + u)$ є найстарший (тобто t-й) розряд суми цілих чисел, які відповідають зазначеним двійковим векторам довжини t, а $x_i \overset{t}{+} y_i \overset{t}{+} u$ є сумою цих чисел за модулем 2^t.

Твердження 4.3. Параметр (4.12) задовольняє такій рівності:

$$l_{\alpha,\beta}(s) = \left| (1,\,0)\; A^{(0)}_{\alpha_0,\beta_0} A^{(1)}_{\alpha_1,\beta_1} \cdots A^{(p-1)}_{\alpha_{p-1},\beta_{p-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right|, \tag{4.14}$$

Крім того, справедлива нерівність

$$l_{\alpha,\beta}(s) \le n_{\alpha_0,\beta_0}(s_0)\, n_{\alpha_1,\beta_1}(s_1) \cdots n_{\alpha_{p-1},\beta_{p-1}}(s_{p-1}), \tag{4.15}$$

де

$$n_{\alpha_i,\beta_i}(s_i) = \left\| A^{(i)}_{\alpha_i,\beta_i} \right\|_\infty =$$

$$= \max\{|\, A^{(i)}_{\alpha_i,\beta_i}(0,0)\,| + |\, A^{(i)}_{\alpha_i,\beta_i}(0,1)\,|, |\, A^{(i)}_{\alpha_i,\beta_i}(1,0)\,| + |\, A^{(i)}_{\alpha_i,\beta_i}(1,1)\,|\}, \; i \in \overline{0,\, p-1}. \tag{4.16}$$

Доведення. На підставі тверджень 4.1 і 4.2 достатньо переконатися в тому, що відображення $F(x,y) = ((x \overset{pt}{+} y) \oplus x,\, s(y))$, $x, y \in V_t{}^p$ (множини $V_t{}^p \times V_t{}^p$ у себе) реалізується послідовністю скінченних автоматів (X, U, V_{2t}, h_i, f_i), де $X = V_{2t}$, $U = \{0,1\}$, а функції h_i, f_i для кожного $i \in \overline{0,\, p-1}$ визначаються таким чином:

$$h_i(u,(x_i,y_i)) = \mathrm{msb}(u + x_i + y_i),\; u \in U,\; (x_i,y_i) \in X,$$

$$f_i(u,(x_i,y_i)) = ((u \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i,\ s_i(y_i)),\ u \in U,\ (x_i,y_i) \in X\ .$$

Дійсно, позначимо $z = (z_0,...,z_{p-1}) = (x \overset{pt}{+} y) \oplus x$ та покладемо

$$u_0 = 0,\ u_{i+1} = h_i(u_i,(x_i,y_i)),\ z_i' = (u_i \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i,\ i \in \overline{0,\ p-1}.$$

За допомогою індукції по i неважко переконатися в тому, що $z_i = z_i'$ для кожного $i \in \overline{0,\ p-1}$. Звідси випливає, що відображення F співпадає з відображенням (4.1) для зазначених вище функцій h_i, f_i, фіксованого значення $u_0 = 0$ та $n = p$, що і треба було довести.

Таким чином, твердження повністю доведено.

4.1.2. Застосування теоретико-автоматного підходу до оцінювання стійкості ординарних модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак. Розглянемо ординарний модулярний SNOW 2.0-подібний шифр, який отримується в результаті заміни операції $*$ у схемі на рис. 2.1 операцією $\overset{r}{+}$ додавання двійкових цілих чисел за модулем 2^r, а підстановка σ визначається за формулою (2.3). На підставі співвідношень (2.12), (2.13), стійкість цього шифру відносно кореляційних атак над полем порядку $2^{r'}$ залежить від параметра (2.24). Наступне твердження встановлює верхню оцінку цього параметра.

Твердження 4.4. Для ординарного модулярного SNOW 2.0-подібного шифру параметр (2.24) задовольняє такій нерівності:

$$\Delta_{c,r'}(k) \le (2^{r'}-1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}, \qquad (4.17)$$

де

$$n_{\max} = \max\{ n_{\alpha_i,\beta_i}(s_i) : (\alpha_i,\beta_i) \in V_t \times V_t \setminus \{(0,0)\}, i \in \overline{0,\, p-1}\},$$

$n_{\alpha_i,\beta_i}(s_i)$ визначається за формулою (4.16), $i \in \overline{0,\, p-1}$, а $B(D^T)$ – за формулою (3.1).

Доведення. З твердження 2.2 випливає, що

$$\Delta_{c,r'}(k) \le (2^{r'}-1)\left(\max_{\alpha \in F_{2^r} \setminus \{0\}} |\hat{\pi}(\alpha)| \right)^{2k}, \qquad (4.18)$$

де $\hat{\pi}(\alpha)$ є коефіцієнтом Фур'є розподілу випадкової величини (2.5):

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\} (-1)^{\mathrm{Tr}_2^{2^r}(\alpha x)}, \ \alpha \in F_{2^r} \setminus \{0\}.$$

Згідно з формулою (2.5), випадкова величина ξ_i є сумою двох незалежних випадкових величин:

$$\xi_{1,i} = (x_{i+n-1} \overset{r}{+} u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)$$

та

$$\xi_{2,i} = (x_{i+n} \overset{r}{+} x_{i+\mu} \overset{r}{+} v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i),$$

де $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ є незалежними випадковими величинами з рівномірним розподілом на множині V_r. Отже на підставі теореми про згортку (дивю, наприклад, [6]) коефіцієнти Фур'є розподілу ξ_i є добутками коефіцієнтів Фур'є розподілів $\xi_{1,i}$ та $\xi_{2,i}$, тобто $\hat{\pi}(\alpha) = \hat{\pi}_1(\alpha)\hat{\pi}_2(\alpha)$, де

$$\hat{\pi}_1(\alpha) = \sum_{z \in F_{2^r}} \mathbf{P}\{\xi_{1,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)}, \ \hat{\pi}_2(\alpha) = \sum_{z \in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)}.$$

Звідси випливає, що

$$|\hat{\pi}(\alpha)| \le |\hat{\pi}_2(\alpha)| = \left| \sum_{z \in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)} \right| = 2^{-2r} \left| \sum_{x,y \in F_{2^r}} (-1)^{\mathrm{Tr}_2^{2^r}(((\overset{r}{x+y}) \oplus x \oplus \sigma(y))\alpha)} \right|.$$

Далі, використовуючи формулу (2.3) та пару дуальних базисів B, $\hat{\mathrm{B}}$ поля F_{2^r} над підполем F_{2^t} як у доведенні твердження 3.1, отримаємо, що

$$\mathrm{Tr}_2^{2^r}(((\overset{r}{x+y}) \oplus x \oplus \sigma(y))\alpha) = \mathrm{Tr}_2^{2^t}(((\overset{r}{x+y}) \oplus x) \cdot \hat{\alpha} \oplus s(y) \cdot \hat{\beta}) \qquad (4.19)$$

де елементи $(\overset{r}{x+y}) \oplus x$ та $s(y) = (s_0(y_0), \ldots, s_{p-1}(y_{p-1}))$ поля F_{2^r} ототожнюються з наборами їх координат у базисі B, $\hat{\alpha} = (\hat{\alpha}_0, \ldots, \hat{\alpha}_{p-1})$ є набором координат елемента α в базисі $\hat{\mathrm{B}}$, $\hat{\beta} = \hat{\alpha}D^T$, а символ $\cdot$ позначає скалярний добуток векторів над полем F_{2^t}. Нарешті, вираз у правій частині рівності (4.19) співпадає з булевим скалярним добутком $((\overset{r}{x+y}) \oplus x)\hat{\alpha} \oplus s(y)\hat{\beta}$, якщо

ототожнити координати векторів $(x \overset{r}{+} y) \oplus x$ та $s(y)$ над полем F_{2^t} з наборами їх координат у певному базисі цього поля над підполем F_2, а координати векторів $\hat{\alpha}$ та $\hat{\beta}$ – з наборами їх координат у відповідному дуальному базисі.

Таким чином, з точністю до зазначеного ототожнення, справедлива така нерівність:

$$|\hat{\pi}(\alpha)| \le 2^{-2tp} \left| \sum_{x,y \in F_{2^t}{}^p} (-1)^{\overset{pt}{((x \overset{r}{+} y) \oplus x)\hat{\alpha} \oplus s(y)\hat{\beta}}} \right|, \qquad (4.20)$$

де $\hat{\alpha} = (\hat{\alpha}_0, \dots, \hat{\alpha}_{p-1}) \in F_{2^t}{}^p$, $\hat{\beta} = \hat{\alpha} D^T$, а $((x \overset{r}{+} y) \oplus x)\hat{\alpha}$ та $s(y)\hat{\beta}$ позначають булеві скалярні добутки зазначених двійкових векторів.

З отриманої нерівності на підставі твердження 4.3 випливає оцінка

$$|\hat{\pi}(\alpha)| \le n_{\hat{\alpha}_0, \hat{\beta}_0}(s_0)\, n_{\hat{\alpha}_1, \hat{\beta}_1}(s_1) \cdots n_{\hat{\alpha}_{p-1}, \hat{\beta}_{p-1}}(s_{p-1}),$$

яка, у свою чергу, тягне оцінку $|\hat{\pi}(\alpha)| \le (n_{\max})^l$, де

$l = |\{i \in \overline{0, p-1} : (\hat{\alpha}_i, \hat{\beta}_i) \ne (0,0)\}|$.

Далі, використовуючи рівність $\hat{\beta} = \hat{\alpha} D^T$ та формулу (3.1), отримаємо, що $B(D^T) \le wt(\hat{\alpha}) + wt(\hat{\beta}) \le l + l = 2l$. Отже, для будь-якого $\alpha \in F_{2^r} \setminus \{0\}$ справедлива нерівність $|\hat{\pi}(\alpha)| \le (n_{\max})^{\left\lceil \frac{B(D^T)}{2} \right\rceil}$, з якої внаслідок формули (4.18) випливає нерівність (4.17).

Твердження доведено.

Отримані твердження, поряд зі співвідношеннями (2.11) – (2.13), складають наукову основу методу обґрунтування стійкості ординарних модулярних SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полем порядку $2^{r'}$ безпосередньо за параметрами їх компонент (див. формули (3.1), (4.13), (4.16)). При цьому застосування замість параметра $\Delta_{c,r'}(k)$ його верхньої оцінки (4.17) у формулах (2.11) – (2.13) надає можливість отримувати нижні оцінки середньої трудомісткості та обсягу матеріалу, потрібного для проведення на шифр будь-якої з (наведених вище) кореляційних атак над полем порядку $2^{r'}$.

4.2. Формальний опис запропонованого методу

Метод призначений для отримання нижніх оцінок параметрів (2.12), (2.13), які визначають, відповідно, середню трудомісткість та обсяг матеріалу, потрібного для проведення на ординарний модулярний SNOW 2.0-подібний потоковий шифр будь-якої з кореляційних атак над полем порядку $2^{r'}$, описаних в п. 2.2.

На відміну від раніше відомих [1 – 4, 5, 7, 8], запропонований метод є застосовним до модулярних r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування.

Сутність методу полягає в побудові верхніх оцінок параметра (2.22), виходячи з матричного представлення параметра (2.27), яке, у свою чергу, отримується на основі теоретико-автоматного опису розподілу ймовірностей випадкових величин (2.5).

Алгоритм реалізації методу наведено на рис. 4.1.

Зауважимо, що для обчислення параметра $n_{\max}$ на кроці 1 алгоритму 4.1 можна використовувати алгоритм 4.2 (рис. 4.2), коректність якого випливає з

формул (4.13), (4.16). Застосування швидкого перетворення Адамара (див., наприклад, [9], с. 217) на кроці 2 алгоритму 4.2 дозволяє скоротити часову складність обчислення значення $n_{\max}$ до $(2t+1)p2^{2t+2}$ операцій замість $6p2^{4t}$ операцій, що використовуються при застосуванні звичайного алгоритму, який базується на формулі (4.13).

Дійсно, для обґрунтування коректності алгоритму 4.2 достатньо переконатися в тому, що $A'^{(s_i)}_{a,b}(u,u') = A^{(s_i)}_{a,b}(u,u')$ для будь-яких $a, b \in V_t$, $u, u' \in \{0,1\}$, $i \in \overline{0,\ p-1}$. Використовуючи формулу (4.13), отримаємо, що

$$A^{(s_i)}_{a,b}(u,u') = 2^{-2t} \sum_{z_1, z_2 \in V_t : \operatorname{msb}(x+z_1+z_2)=u'} (-1)^{(z_1 \overset{t}{+} z_2 \overset{t}{+} u)a \oplus z_1 a \oplus s_i(z_2) b} =$$

$$= 2^{-2t} \sum_{x,y \in V_t} \sum_{\substack{z_1, z_2 \in V_t : \\ \operatorname{msb}(z_1 \overset{t}{+} z_2 \overset{t}{+} u)=u', \\ (u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1 = x, \\ s_i(z_2)=y\}|}} (-1)^{(z_1 \overset{t}{+} z_2 \overset{t}{+} u)a \oplus z_1 a \oplus s_i(z_2) b} =$$

$$= 2^{-2t} \sum_{x,y \in V_t} \sum_{\substack{z_1, z_2 \in V_t : \\ \operatorname{msb}(z_1 \overset{t}{+} z_2 \overset{t}{+} u)=u', \\ (u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1 = x, \\ s_i(z_2)=y\}|}} (-1)^{xa \oplus s_i(y) b} = 2^{-2t} \sum_{x,y \in V_t} \sum_{\substack{z_1, z_2 \in V_t : \\ \operatorname{msb}(z_1 \overset{t}{+} z_2 \overset{t}{+} u)=u', \\ (u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1 = x, \\ s_i(z_2)=y\}}} (-1)^{xa \oplus yb} =$$

$$= 2^{-2t} \sum_{x,y \in V_t} D^{(s_i)}_{u,u'}(x,y)(-1)^{xa \oplus yb} = A'^{(s)}_{a,b}(u,u').$$

Отже, на підставі формули (4.16) алгоритм 4.2 дійсно обчислює значення $n_{\max}$.

Далі, при фіксованому $i \in \overline{0,\, p-1}$ на кроці 1 для обчислення усіх значень $D_{u,u'}^{(s_i)}(x,\, y)$ побудуємо масив (спочатку заповнений нулями), адресами елементів якого є трійки (u', x, y), де $u' \in \{0,1\}$, $x,\, y \in V_t$. Для кожного $u \in \{0,1\}$ всі значення $D_{u,u'}^{(s_i)}(x,\, y)$ можна обчислити в одному циклі по (z_1, z_2), додаючи 1 до поточного значення елемента масиву, який зберігається за адресою (u', x, y), де $u' = \mathrm{msb}(u + z_1 + z_2)$, $x = (u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1, y = s_i(z_2)$. Зрозуміло, що для цього достатньо виконати $4 \cdot 2^{2t}$ операцій (обчислення суми $u + z_1 + z_2$, додавання за модулем 2 при обчисленні x, звернення до підстановки s_i при обчисленні y та додавання 1 до поточного елемента масиву). На кроці 2 застосування швидкого перетворення Адамара до функції $D_{u,u'}^{(s_i)}(x,\, y)$, $x,\, y \in V_t$ потребує $2t2^{2t}$ операцій для кожної пари значень $u, u' \in \{0,1\}$. Отже, часова складність цього кроку складає $8t2^{2t}$ операцій, а часова складність алгоритму 4.2 в цілому дорівнює $(2t+1)p2^{2t+2}$.

Зауважимо, що при $t = 8$ виграш у трудомісткості при застосуванні алгоритму 4.2 в порівнянні з тривіальним алгоритмом складає $\dfrac{6 \cdot 2^{4t}}{(2t+1)2^{2t+2}} > 2^{11}$.

Приклади застосування методу. Отримаємо нижні оцінки параметрів, що визначають ефективність кореляційних атак над полем $F_{2^t} = F_{256}$ на шифр SNOW 2.0.

Нагадаємо (див. приклад 2.1), що параметри цього шифру мають такі значення: $t = 8$, $p = 4$, $n = 16$. При цьому підстановка σ має вигляд (2.3), де підстановки $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0,\, p-1}$, та матриця D задаються так само, як у раундовому перетворенні шифру Rijndaep; зокрема, $B(D^T) = p + 1 = 5$.

Використовуючи алгоритм 4.2, знайдемо, що $n_{\max} = 2^{-3}$. Отже, $(n_{\max})^2 = 2^{-6} = l_{\max}$, де значення $l_{\max}$ обчислено у підрозділі 3.2. Звідси випливає, що результати, отримані за допомогою алгоритму 3.1 для двійкової версії шифру (див. табл. 3.1) співпадають з відповідними результатами, які отримуються за допомогою алгоритму 4.1 для оригінального SNOW 2.0.

Алгоритм 4.2

Вхідні дані: підстановки $s_i : V_t \to V_t$, $i \in \overline{0,\ p-1}$.

Для кожного $i \in \overline{0,\ p-1}$ виконати такі обчислення.

1. Для кожного $u \in \{0,1\}$ підрахувати значення

$$D_{u,u'}^{(s_i)}(x, y) = |\{(z_1, z_2) \in V_t \times V_t : \mathrm{msb}(u + z_1 + z_2) = u',$$
$$(u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1 = x,\ s_i(z_2) = y\}|$$

для усіх $u' \in \{0,1\}$, $x, y \in V_t$;

2. Для усіх $u, u' \in \{0,1\}$ обчислити значення

$$A'^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{x,y \in V_t} D_{u,u'}^{(s_i)}(x,y)(-1)^{xa \oplus yb},\ a, b \in V_t,$$

за допомогою алгоритму швидкого перетворення Адамара.

3. Для кожної пари $(a, b) \in V_t \times V_t \setminus \{(0, 0)\}$ обчислити

$$n_{a,b}(s_i) = \max\{|A'^{(i)}_{a,b}(0,0)| + |A'^{(i)}_{a,b}(0,1)|, |A'^{(i)}_{a,b}(1,0)| + |A^{(i)}_{a,b}(1,1)|\}.$$

4. Обчислити

$$n_{\max}(s_i) = \max\{n_{a,b}(s_i) : (a,b) \in V_t \times V_t \setminus \{(0,0)\}\},$$

Результат:

$$n_{\max} = \max_{i \in \overline{0,\ p-1}} \{n_{\max}(s_i)\}.$$

Рис. 4.2. Швидкий алгоритм обчислення параметра $n_{\max}$

Таким чином, згідно з табл. 3.1, будь-яка з (розглянутих вище) кореляційних атак над полем порядку 256 на шифр SNOW 2.0 має середню часову складність не менше ніж $2^{146,20}$ та потребує не менше ніж $2^{142,77}$ знаків гами.

Розглянемо зараз шифр “Струмок” (приклад 2.2), де використовуються такі параметри: $t=8$, $p=8$, $n=16$. При цьому підстановка σ має вигляд (2.3), де вузли заміни та матриця D задаються так само, як у блоковому шифрі “Калина”. Зокрема, у “Струмку” застосовується чотири різні підстановки π_0, π_1, π_2, π_3 (кожна з яких використовується двічі); при цьому $B(D^T)=p+1=9$ [10, 11].

В табл. 4.1 наведені значення параметра $n_{\max}(\pi_i)$, $i\in\overline{0,3}$, а також векторів a,b, на яких досягається максимум у виразі цього параметра (див. крок 4 алгоритму 4.2). Згідно з таблицею, $(n_{\max})^2=(3\cdot 2^{-4})^2=l_{\max}$, де значення $l_{\max}$ обчислено у підрозділі 3.2. Отже, результати, отримані за допомогою алгоритму 3.1 для двійкової версії шифру “Струмок” (див. табл. 3.2) співпадають з відповідними результатами, які отримуються за допомогою алгоритму 4.1 для оригінального шифру.

Таблиця 4.1

Результати застосування алгоритму 4.2 для вузлів заміни шифру “Струмок”

Підстановка π, що використовується у шифрі “Калина”	$n_{\max}(\pi)$	a	b
π_0	$3\cdot 2^{-4}$	1 = (0000 0001)	212 = (1101 0100)
π_1	$11\cdot 2^{-6}$	1 = (0000 0001)	244 = (1111 0100)
π_2	$5\cdot 2^{-5}$	1 = (0000 0001)	20 = (0001 0100)
π_3	$5\cdot 2^{-5}$	1 = (0000 0001)	190 = (1011 1110)

Алгоритм 4.1

Вхідні дані:

– натуральні числа n, p, t;

– підстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$;

– оборотна $p \times p$-матриця D над полем F_{2^t}.

– число $k \geq 2$, що є степенем двійки;

–дільник r' числа r;

– допустима верхня межа δ ймовірності помилки атаки.

1. Обчислити значення $\Delta_{r'}(k) = (2^{r'} - 1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}$, використовуючи формули (3.1), (4.13), (4.16).

2. Покласти $r'' = pt(r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.

3. Для кожного $l' = 1, 2, ..., l-1$ обчислити

$$m_{r'}(k) = (\Delta_{r'}(k))^{-1}((1-\delta)l'r' - h(\delta))\ln 2,$$

$$T_{r'}(k, l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r'l'2^{r'l'}) + 2^{r'(l'+1)}.$$

4. Обрати $l^* \in \overline{1, l-1}$ таке, що $T_{r'}(k, l^*) = \min\{T_{r'}(k, l') : l' \in \overline{1, l-1}\}$.

Результат:

– число l^* фрагментів (довжини r' бітів кожний) початкового стану генератора, які відновлюються за допомогою атаки;

– середня часова складність атаки $T_{r'}(k, l^*)$;

– обсяг матеріалу

$$N_{r'}(k, l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}},$$

потрібного для успішної реалізації атаки.

Рис. 4.1. Алгоритм реалізації методу обґрунтування стійкості ординарних модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак

Таким чином, будь-яка з (розглянутих вище) кореляційних атак над полем порядку 256 на шифр “Струмок” має середню часову складність не менше ніж $2^{249,40}$ та потребує не менше ніж $2^{249,38}$ знаків гами.

В цілому, отримані результати свідчать про практичну стійкість шифрів SNOW 2.0 та “Струмок” до розглянутих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

4.3. Експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак

Розроблений метод дозволяє отримати відповідь на запитання про те, наскільки великою є частка вузлів заміни (серед усіх підстановок на множині V_t), які при фіксованих значеннях решти параметрів ординарного модулярного SNOW 2.0-подібного шифру забезпечують його стійкість відносно розглянутих кореляційних атак на рівні заданого порогу. Методологія дослідження підстановок, викладена в підрозділі 3.3, залишається незмінною і для випадку модулярних шифрів, що дозволяє оцінити середній час, який потрібно витратити на формування довгострокових ключів ординарного двійкового SNOW 2.0-подібного шифру (принаймні, виходячи з критерію його стійкості відносно кореляційних атак).

На підставі тверджень 2.1, 2.2 і 4.4 поставлене запитання зводиться до наступного.

Для будь-якої підстановки s на множині V_t позначимо $n_{\max}(s)$ максимум значень вигляду (4.16) за всіма ненульовими елементами $a_j, b_j \in F_{2^t}$. Для

кожного $x \in (0,1)$ позначимо $F(x)$ відносне число (частку) тих підстановок s (серед усіх можливих на множині V_t), для яких $n_{\max}(s) < x$. Треба побудувати статистичну оцінку параметра $F(x)$ із заданими точністю ε та достовірністю $1-\delta$, де $\varepsilon, \delta \in (0,1)$.

Для розв'язання цієї задачі скористаємося алгоритмом 4.3 (рис. 4.3), який базується на методі Монте-Карло, а також на відомому алгоритмі швидкого перетворення Адамара (див., наприклад, [9]).

На підставі нерівності Чернова (див., наприклад, [12]), значення $F(x)$, яке треба оцінити, знаходиться в інтервалі $(F_N(x)-\varepsilon, F_N(x)+\varepsilon)$ з ймовірністю не менше ніж $1-\delta$, де $F_N(x)$ є результатом виконання алгоритму 3.2.

В табл. 4.2 наведено результати, отримані на перших трьох кроках алгоритму 4.3 при $t = 8$, $\varepsilon = 0{,}037$, $\delta = 0{,}01$.

У другій колонці табл. 4.2 показані точні значення $n_{\max}(s_i)$, отримані для $N = \left\lceil 1/2 \cdot \varepsilon^{-2} \ln(2\delta^{-1}) \right\rceil = 2000$ випадкових рівноймовірних підстановок $s_i : V_t \to V_t$, а в першій колонці – кількість $N(n_{\max})$ підстановок із заданим значенням параметра $n_{\max}$. Результати в останніх трьох колонках табл. 4.2 отримано за допомогою алгоритму 4.1 при тих самих вхідних даних, що й для шифру "Струмок": $t = 8$, $p = 8$, $n = 16$, $B(D^T) = p+1 = 9$, $r' = t$, $\delta = 0{,}01$. Обчислення проведено в macOS Mojave 10.14, 2.2 GHz Intel Core i7, 16 GB 2400 MHz DDR4, Intel UHD Graphics 630 1536 MB).

На рис. 4.4 показано гістограму емпіричного розподілу ймовірностей випадкової величини $n_{\max}(s)$, де s є випадковою рівноймовірною підстановкою на множині V_t при $t = 8$.

Алгоритм 4.3

Вхідні дані:

– натуральне число t;

– підстановка $s: F_{2^t} \to F_{2^t}$;

– числа $\varepsilon, \delta \in (0,1)$;

– число $x \in (0,1)$.

1. Обчислити $N = \left\lceil 1/2 \cdot \varepsilon^{-2} \ln(2\delta^{-1}) \right\rceil$.

2. Згенерувати незалежні випадкові рівноймовірні підстановки $s_1, ..., s_N$.

3. Для кожного $i \in \overline{1, N}$ обчислити значення $n_{\max}(s_i)$, використовуючи наступну процедуру.

3.1. Для кожного набору $a \in V_t$, $u, u' \in \{0,1\}$ обчислити:

– обчислити значення функції

$$f^{(i)}_{a,\,u,u'}(z) = \sum_{x \in V_t:\ \mathrm{msb}(x + s_i^{-1}(z) + u) = u'} (-1)^{(\overset{t}{x} + s_i^{-1}(z) + \overset{t}{u})a \,\oplus\, xa},\ z \in V_t;$$

– обчислити

$$A^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{z \in V_t} f^{(i)}_{a,\,u,u'}(z)(-1)^{zb},\ b \in V_t$$

за допомогою алгоритму швидкого перетворення Адамара;

– для кожної пари $(a,b) \in V_t \times V_t \setminus \{(0,0)\}$ обчислити

$$n_{a,b}(s_i) = \max\{|A^{(i)}_{a,b}(0,0)| + |A^{(i)}_{a,b}(0,1)|, |A^{(i)}_{a,b}(1,0)| + |A^{(i)}_{a,b}(1,1)|\}.$$

3.2. Покласти $n_{\max}(s_i) = \max\{n_{a,b}(s_i) : (a,b) \in V_t \times V_t \setminus \{(0,0)\}\}$.

4. Підрахувати число $F_N(x)$ таких значень $i \in \overline{1, N}$, для яких $n_{\max}(s_i) < x$.

Результат: значення $F_N(x)$.

Рис. 4.3. Алгоритм статистичного оцінювання розподілу параметра $n_{\max}(s)$ як функції випадкової рівноймовірної підстановки s

Таблиця 4.2

Значення параметрів, що визначають стійкість ординарних модулярних SNOW 2.0-подібних шифрів з випадково згенерованими вузлами заміни

$N(n_{\max})$	$n_{\max}$	k	$l*$	$\log T_{r'}(k,l*)$	$\log N_{r'}(k,l*)$
575	0,1875	2	24	348,44	347,36
		4	31	263,45	263,38
		8	29	249,40	249,38
		16	21	181,55	181,34
473	0,171875	2	44	364,27	362,87
		4	34	286,85	286,73
		8	30	251,61	249,91
		16	1	404,97	287,59
453	0,203125	2	44	363,74	360,46
		4	34	284,39	283,52
		8	29	247,16	247,07
		16	1	366,40	279,88
206	0,21875	2	43	363,38	363,38
		4	34	283,78	282,09
		8	29	245,28	244,94
		16	1	349,30	276,46
117	0,15625	2	44	364,95	364,25
		4	34	288,60	288,56
		8	30	253,08	252,66
		16	1	426,97	291,99
80	0,234375	2	43	362,40	362,38
		4	33	283,42	283,42
		8	29	243,99	242,95

		16	1	333,37	273,27
31	0,25	2	43	361,48	361,45
		4	33	282,19	282,17
		8	28	243,08	243,07
		16	1	318,48	270,30
14	0,1796875	2	44	364,06	362,23
		4	34	286,09	285,87
		8	29	250,62	250,61
		16	1	394,71	285,54
13	0,265625	2	43	360,62	360,58
		4	33	281,03	281,01
		8	28	241,34	241,32
		16	1	304,48	267,47
9	0,1640625	2	44	364,57	363,545
		4	34	287,69	287,62
		8	30	252,17	251,25
		16	1	415,71	289,74
5	0,17578125	2	44	364,16	362,55
		4	34	286,46	286,230
		8	29	251,25	251,25
		16	1	399,78	286,56
3	0,177734375	2	44	364,11	362,39
		4	34	286,27	286,08
		8	29	250,93	250,93
		16	1	397,23	286,05
3	0,1953125	2	44	363,81	361,03
		4	34	284,85	284,27

		8	29	248,25	248,21
		16	1	375,46	281,69
2	0,16015625	2	44	364,75	363,89
		4	34	288,14	288,09
		8	30	252,58	251,94
		16	1	421,27	290,85
2	0,18359375	2	44	363,98	361,92
		4	34	285,74	285,46
		8	29	250,00	249,99
		16	1	389,74	284,55
1	0,140625	2	44	366,06	365,77
		4	34	290,60	290,59
		8	30	255,76	255,70
		16	1	451,29	296,86
1	0,14453125	2	44	365,74	365,37
		4	34	290,07	290,06
		8	30	255,00	254,91
		16	1	444,96	295,59
1	0,1611328125	2	44	364,70	363,80
		4	34	288,02	287,97
		8	30	252,47	251,77
		16	1	419,87	290,57
1	0,166748046875	2	44	364,45	363,31
		4	34	287,40	287,31
		8	30	251,94	250,78
		16	1	411,96	288,99
1	0,16796875	2	44	364,41	363,21

		4	34	287,26	287,17
		8	30	251,85	250,57
		16	1	410,27	288,65
1	0,173828125	2	44	364,21	362,71
		4	34	286,65	286,51
		8	30	251,52	249,58
		16	1	402,36	287,07
1	0,17431640625	2	44	364,20	362,67
		4	34	286,61	286,46
		8	29	251,49	251,49
		16	1	401,71	286,94
1	0,193359375	2	44	363,83	361,17
		4	34	284,98	284,46
		8	29	248,53	248,50
		16	1	377,78	282,16
1	0,21484375	2	43	363,64	363,63
		4	34	283,90	282,44
		8	29	245,70	245,46
		16	1	353,46	353,46
1	0,2421875	2	43	361,93	361,91
		4	33	282,79	282,78
		8	29	243,61	242,00
		16	1	325,81	271,76
1	0,28125	2	43	359,83	359,75
		4	33	279,96	279,91
		8	28	239,73	239,67
		16	1	291,29	264,86

1	0,34375	2	43	357,35	356,86
		4	33	276,69	276,05
		8	28	235,57	233,88
		16	8	248,14	244,99

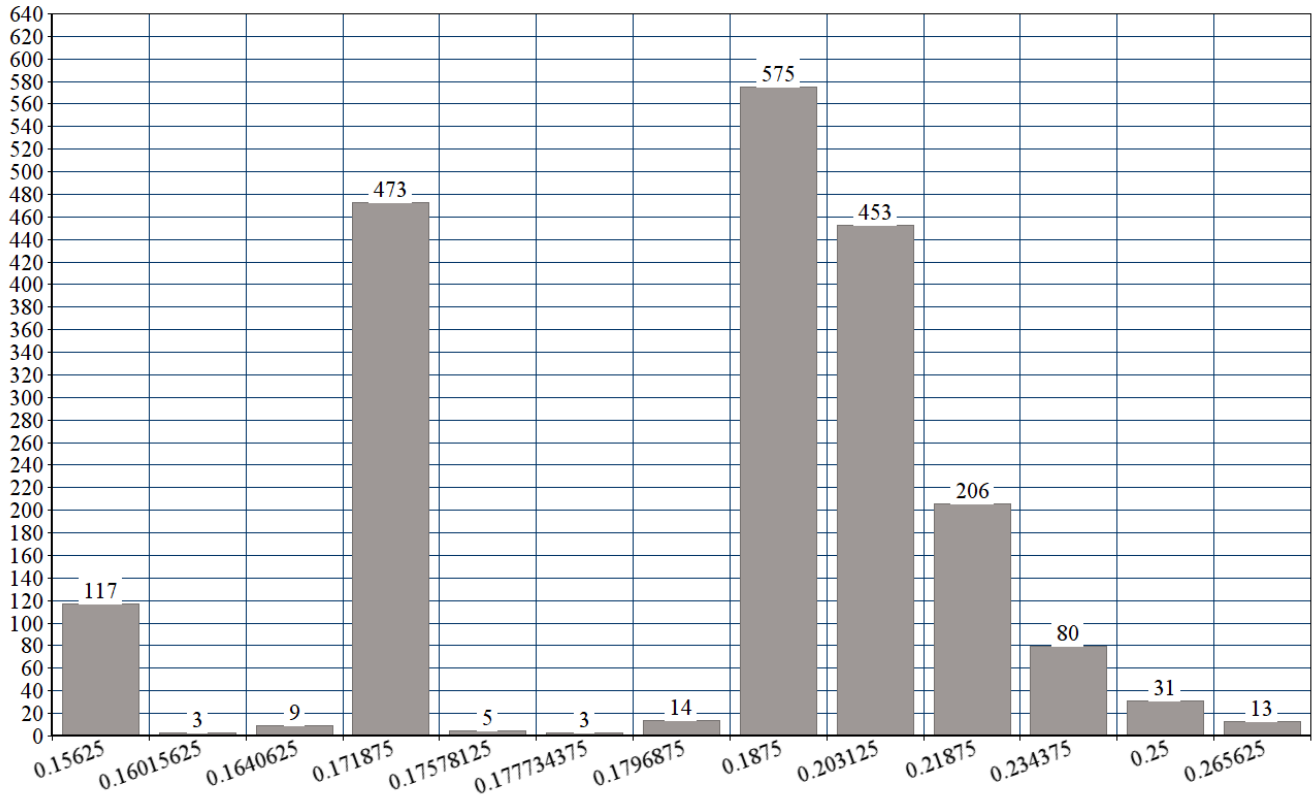

Рис. 4.4. Гістограма, побудована за виборкою з 2000 випадкових рівноймовірних підстановок

Як видно з рис. 4.4 і табл. 4.2, при $x = 0{,}19$ умова $n_{\max}(s) < x$ виконується для $575+14+3+5+473+9+3+117=1199$ з $N = 2000$ випадково згенерованих підстановок s. При цьому середня трудомісткість кореляційної атаки на SNOW 2.0-подібний шифр з такими підстановками є не менше ніж $2^{251,25}$.

Отже, $F_N(x) = \dfrac{1199}{2000} = 0{,}5995$ і з достовірністю принаймні $1-\delta$ (тобто 99 %) відносне число всіх підстановок, які забезпечують стійкість шифру до кореляційних атак на рівні не менше ніж $2^{251{,}25}$, знаходиться в межах від $0{,}5995-\varepsilon$ до $0{,}5995+\varepsilon$. Іншими словами, майже 60% випадково згенерованих підстановок забезпечують стійкість відповідного SNOW 2.0-подібного шифру на рівні $2^{251{,}25}$.

При $x = 0{,}266$ маємо $F_N(x) = 1$; при цьому, оскільки найменше значення $\log T_{r'}(k, l^*)$ у четвертій колонці табл. 4.2 дорівнює 235,57, то середня трудомісткість атаки на шифр є не менше ніж $2^{235{,}57}$. Таким чином, з достовірністю принаймні 99 % частка підстановок, які забезпечують зазначену стійкість SNOW 2.0-подібних шифрів, складає не менше ніж $1-\varepsilon$.

В цілому, отримані результати показують, що при використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\, p-1}$, в ролі довгострокових ключових параметрів ординарних модулярних SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість шифрів відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу.

Висновки

1. Основним науковим результатом розділу є метод обґрунтування стійкості модулярних SNOW 2.0-побдібних потокових шифрів відносно кореляційних атак, описаних в розділі 2. Метод базується на отриманих дисертантом твердженнях 4.1, 4.2 і 4.3, перше з яких надає матричне представлення для незбалансованості довільного дискретного відображення, яке реалізується послідовністю скінченних автоматів і узагальнює низку окремих

результатів про матричні (або лінійні) представлення незбалансованості відображень, що реалізуються автоматами спеціального вигляду [1, 5]. Останні два твердження містять верхні оцінки незбалансованості, які можуть бути використані на практиці для обґрунтування стійкості ординарних модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак.

2. На відміну від раніше відомих [1 – 4, 5, 7, 8], запропонований метод є застосовним до модулярних r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування. Сутність методу полягає в побудові верхніх оцінок параметра (2.22), виходячи з матричного представлення параметра (2.27), яке, у свою чергу, отримується на основі теоретико-автоматного опису розподілу ймовірностей випадкових величин (2.5).

3. Твердження 4.4 встановлює нижні межі трудомісткості та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на ординарні модулярні SNOW 2.0-подібні шифри. Застосування отриманих меж до шифрів SNOW 2.0 та “Струмок” приводить до результатів, які співпадають з результатами, отриманими для їх двійкових версій: будь-яка кореляційна атака на зазначені шифри (з визначеного класу атак) над полем порядку 256 має середню трудомісткість не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно, $2^{249,38}$ знаків гами. Це свідчить про практичну стійкість шифрів SNOW 2.0 та “Струмок” відносно відомих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

4. Вирази отриманих меж трудомісткості та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на ординарні модулярні SNOW 2.0-подібні шифри, залежать від параметрів вигляду (4.16), які можна розглядати як

модифіковані елементи таблиць лінійних апроксимацій вузлів заміни, а також від індексу галуження лінійного перетворення у схемі алгоритму шифрування. Запропонований алгоритм 4.2 дозволяє скоротити (не менш як у 2^{11} разів) час обчислення зазначених параметрів у порівнянні зі звичайним алгоритмом, який базується на формулі (4.13).

5. При використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, в ролі довгострокових ключових параметрів ординарних модулярних SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу. Зокрема, з достовірністю принаймні 99 % відносне число всіх підстановок, які забезпечують стійкість шифру відносно кореляційних атак на рівні не менше ніж $2^{251,25}$, знаходиться в межах від 0,5625 до 0,6365. При цьому з достовірністю принаймні 99 % частка тих підстановок, які забезпечують стійкість на рівні не менше ніж $2^{235,57}$, складає щонайменше 0,963.

Список використаних джерел у четвертому розділі

13. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption. FSE 2006. LNCS 4047. Springer-Verlag*. 2006. P. 144 – 162.

14. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology. ASIACRYPT 2005. LNCS 3788. Springer-Verlag*. 2005. P. 313 – 332.

15. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive, Report 2016/311*. URL: http://eprint.iacr.org/2016/311 (дата звернення: 27.01.2020)

16. Жуков А.Е., Чистяков В.П. Матричный подход к исследованию прообразов выходной последовательности конечного автомата. *Обозрение прикл. промышл. матем*. 1994. Т. 1. Вып. 1. С. 108 – 117.

17. Wallén J. Linear approximation of addition modulo 2^n. *Fast Software Encryption. FSE 2003. LNCS 2887. Springer-Verlag.* 2003. P. 261 – 273.

18. Carlet C. Boolean functions for cryptography and error correcting codes. *In Boolean Methods and Models, Cambridge, U.K. Cambridge Univ. Press*. 2006.

19. Watanabe D., Biryukov A., de Cannière C. A distinguishing attack of SNOW 2.0 with linear masking method. *Selected Arreas in Cryptography. SAC 2003. LNCS 3006. Springer-Verlag.* 2003. P. 222 – 233.

20. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology. ASIACRYPT 2008. LNCS 5350. Springer-Verlag*. 2008. P. 524 – 538.

21. Логачев О.А. Сальников А.А, Ященко В.В. Булевы функции в теории кодирования и криптологии. *М.: МЦНМО*. 2004. 470 с.

22. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018, 24 – 27 May, 2018, Kyiv, Ukraine.* P. 292 – 299.

23. Національний стандарт України ДСТУ 8845:2919. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. Київ: ДП "УкрНДНЦ", 2019.

24. Hoeffding W. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc.*1963. Vol. 58. № 301. P. 13 – 30.

ВИСНОВКИ

На сьогодні значна увага приділяється створенню та дослідженню криптографічних властивостей слово-орієнтованих потокових шифрів, призначених для ефективної програмної реалізації на 32- або 64-розрядних процесорах. Важливий клас таких шифрів утворюють SNOW 2.0-подібні шифри, прототипом яких є алгоритм потокового шифрування SNOW 2.0, що є на сьогодні міжнародним стандартом. Іншим прикладом SNOW 2.0-подібного шифру є створений в Україні шифр “Струмок”, прийнятий як національний стандарт ДСТУ 8845:2019.

Аналіз існуючих публікацій показує, що найбільш потужними з відомих атак на шифр SNOW 2.0 є кореляційні атаки, сутність яких полягає у складанні та розв’язанні систем лінійних рівнянь зі спотвореними правими частинами, зокрема, систем рівнянь над полями порядку більшого ніж 2. При цьому залишаються не вирішеними задачі, пов’язані з розробкою методів оцінювання та обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак. На сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість зазначених шифрів відносно відомих кореляційних атак безпосередньо за параметрами їх компонент. Крім того, спроба розповсюдити відомі методи оцінювання стійкості шифру SNOW 2.0 відносно відомих кореляційних атак на деякі інші потокові шифри, зокрема, “Струмок”, наштовхується на труднощі, пов’язані з розміром задач, які треба розв’язувати для отримання оцінок.

В дисертаційній роботі вирішено **актуальну наукову задачу** розробки методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак.

Для вирішення поставленої наукової задачі **використано методи** теорії ймовірностей, теорії інформації, лінійної алгебри, теорії скінченних автоматів,

теорії скінченних полів та перетворення Фур'є псевдобулевих функцій. Чисельні розрахунки на обчислювальній системі виконувалися з використанням середовища розробки IntelliJ IDEA (мова програмування Java) з процесором 2.2 GHz Intel Core i7 та обсягом оперативної пам'яті 16 ГБ на базі macOS Mojave 10.14.

Основні наукові та практичні результати, отримані в дисертації.

1. *Удосконалено* аналітичну оцінку інформаційної складності кореляційних атак на потокові шифри. На відміну від раніше відомої (евристичної) оцінки, отримана аналітична оцінка має належне наукове обґрунтування, містить явну залежність від ймовірності помилки атаки та є справедливою для будь-яких кореляційних атак на потокові шифри незалежно від способу побудови або методу розв'язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

2. *Вперше* отримано аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри. На відміну від відомих співвідношень, які визначають квадратичну евклідову незбалансованість, отримане співвідношення встановлює вираз цього параметра в термінах коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Це дозволяє отримувати нижні оцінки трудомісткості й обсягу матеріалу, потрібного для реалізації кореляційних атак на SNOW 2.0-подібні шифри та порівнювати за трудомісткістю та обсягом матеріалу кореляційні атаки, що будуються над полями різних порядків.

3. *Вперше* розроблено метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на полем з двох елементів, розроблений метод базується на отриманому

дисертантом аналітичному співвідношенні для параметра, який характеризує ефективність атаки, та дозволяє обґрунтовувати стійкість двійкових SNOW 2.0-подібних потокових шифрів безпосередньо за параметрами їх компонент.

4. *Отримав подальший розвиток* метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на SNOW 2.0, розроблений метод базується на отриманих дисертантом аналітичних співвідношеннях, які узагальнюють низку окремих результатів про матричні представлення незбалансованості відображень, що реалізуються скінченними автоматами. Розроблений метод є застосовним до модулярних r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування.

Достовірність результатів дисертаційної роботи забезпечується адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

Значення наукових результатів дисертації для теорії полягає в тому, що вони утворюють наукову основу для вирішення задач оцінювання та обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак. Отримані результати мають універсальний характер, що дозволяє використовувати їх в подальшому при дослідженні стійкості більш широкого класу слово-орієнтованих потокових шифрів.

Практичне значення роботи. Розроблено програмні реалізації, які дозволяють в режимі реального часу обчислювати значення нижніх меж трудомісткості та обсягу матеріалу, потрібного для здійснення будь-якої з відомих кореляційних атак на довільний двійковий чи модулярний SNOW 2.0-

подібний шифр з вузлами заміни довжини 8 бітів. Розроблені програми застосовані для обґрунтування стійкості шифру “Струмок”, а також його двійкової версії. Вони можуть бути використані на практиці при дослідженні стійкості інших SNOW 2.0-подібних потокових шифрів у СІТС України.

Крім того, отримані в роботі результати дозволяють:

– ввести науково обґрунтовані параметри вузлів заміни SNOW 2.0-подібних шифрів, що характеризують їх стійкість відносно відомих кореляційних атак;

– скоротити (не менш як у 2^{11} разів) час обчислення зазначених параметрів завдяки застосуванню розробленого дисертантом алгоритму;

– обґрунтувати практичну стійкість національного стандарту потокового шифрування України “Струмок” відносно відомих кореляційних атак (на рівні $2^{249,40}$ операцій за наявності не менше ніж $2^{249,38}$ знаків гами);

– підвищити обґрунтованість експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Висновки та рекомендації по науковому та практичному використанню наукових результатів.

1. Отримана неасимптотична нижня оцінка інформаційної складності кореляційних атак на потокові шифри уточнює раніше відому (евристичну) оцінку та має належне наукове обґрунтування. Вона справедлива для будь-яких кореляційних атак на довільні потокові шифри незалежно від способу побудови або методу розв’язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки.

2. Отримане аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні ПШ, дозволяє звести задачу знаходження нижніх оцінок трудомісткості

будь-якої атаки з визначеного класу до побудови верхніх меж максимуму модулів коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Таким чином, ефективність кореляційних атак на SNOW 2.0-подібні потокові визначається безпосередньо за коефіцієнтами Фур'є розподілу випадкових величин вигляду (2.5).

3. Будь-яка кореляційна атака над полем $F_{2^{r'}}$ (з класу атак, що розглядається) є не більш ніж у $2^{r'}$ разів ефективніше (як за середньою трудомісткістю, так і за обсягом матеріалу) в порівнянні з найкращою кореляційною атакою над полем F_2. Отже, перехід від двійкових кореляційних атак до атак над полями порядку $2^{r'}$ може підвищити ефективність перших не більше ніж в $2^{r'}$ разів.

4. Застосування викладеного у розділі 3 методу до двійкових версій шифрів SNOW 2.0 та "Струмок" доводить, що будь-яка кореляційна атака на них (з визначеного класу) над полем порядку 256 має середню трудомісткість не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно, $2^{249,38}$ знаків гами, що свідчить про практичну стійкість зазначених двійкових шифрів відносно відомих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

5. При використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, в ролі довгострокових ключових параметрів ординарних двійкових SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу. Зокрема, з достовірністю принаймні 99 % відносне число всіх підстановок, які забезпечують стійкість шифру відносно кореляційних атак на рівні не менше

ніж $2^{241,33}$, знаходиться в межах від $0{,}442$ до $0{,}516$. При цьому з достовірністю принаймні 99 % частка тих підстановок, які забезпечують стійкість на рівні не менше ніж $2^{235,55}$, складає щонайменше 0,963.

6. Вирази отриманих меж трудомісткості та обсягу матеріалу, потрібного для успішної реалізації кореляційних атак на ординарні модулярні SNOW 2.0-подібні шифри, залежать від параметрів вигляду (4.16), які можна розглядати як модифіковані елементи таблиць лінійних апроксимацій вузлів заміни, а також від індексу галуження лінійного перетворення у схемі алгоритму шифрування. Запропонований алгоритм 4.2 дозволяє скоротити (не менш як у 2^{11} разів) час обчислення зазначених параметрів у порівнянні зі звичайним алгоритмом, який базується на формулі (4.13).

7. Застосування викладеного у розділі 4 методу до шифрів SNOW 2.0 та "Струмок" приводить до результатів, які співпадають з результатами, отриманими для їх двійкових версій: будь-яка кореляційна атака на зазначені шифри (з визначеного класу атак) над полем порядку 256 має середню трудомісткість не менше ніж $2^{146,20}$ та $2^{249,40}$ відповідно і потребує не менше ніж $2^{142,77}$ та, відповідно, $2^{249,38}$ знаків гами. Це свідчить про практичну стійкість шифрів SNOW 2.0 та "Струмок" відносно відомих кореляційних атак за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

8. При використанні підстановок $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, в ролі довгострокових ключових параметрів ординарних модулярних SNOW 2.0-подібних шифрів ті підстановки, що забезпечують потрібну стійкість відносно розглянутих кореляційних атак, можуть формуватися в режимі реального часу. Зокрема, з достовірністю принаймні 99 % відносне число всіх підстановок, які забезпечують стійкість шифру відносно кореляційних атак на рівні не менше

ніж $2^{251,25}$, знаходиться в межах від 0,5625 до 0,6365. При цьому з достовірністю принаймні 99 % частка тих підстановок, які забезпечують стійкість на рівні не менше ніж $2^{235,57}$, складає щонайменше 0,963.

9. Комп'ютерні програми, розроблені на основі запропонованих методів, дозволяють в режимі реального часу обчислювати значення нижніх меж трудомісткості та обсягу матеріалу, потрібного для реалізації будь-якої з відомих кореляційних атак на довільний двійковий чи модулярний SNOW 2.0-подібний шифр з вузлами заміни довжини 8 бітів.

10. Основні наукові та практичні результати дисертаційної роботи реалізовані в НДР "Корифена", що виконувалася на замовлення Служби зовнішньої розвідки України, та в науково-технічних розробках ЗАО "Інститут інформаційних технологій". Отримані результати можуть використовуватися при проведенні експертних досліджень для отримання науково обґрунтованих висновків про можливість застосування в Україні перспективних алгоритмів потокового шифрування. Подальший розвиток наукових ідей та методів, які лежать в основі дисертаційного дослідження, є актуальним напрямом в галузі кібербезпеки.

ДОДАТКИ

Додаток А

Програмний код реалізації алгоритму статистичного оцінювання розподілу параметрів $n_{\max}(s)$ та $l_{\max}(s)$ як функцій випадкової рівноймовірної підстановки s

Програмна реалізація виконана на ПК з процесором Intel(R) Core(TM) i7, 2.2 GHz та обсягом оперативної пам'яті 16 ГБ на базі ОС macOS Mojave 10.14. Мова програмування – Java. Середовище розробки Intelij Idea.

```
// Файл main.java


import java.io.BufferedWriter;
import java.io.File;
import java.io.FileWriter;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.HashSet;
import java.util.List;
import java.util.Set;

public class Main {
    public static int [][] sBox =
                      {{0xA4, 0xA2, 0xA9, 0xC5, 0x4E, 0xC9, 0x03, 0xD9, 0x7E, 0x0F, 0xD2,
0xAD, 0xE7, 0xD3, 0x27, 0x5B},
                      {0xE3, 0xA1, 0xE8, 0xE6, 0x7C, 0x2A, 0x55, 0x0C, 0x86, 0x39, 0xD7, 0x8D,
0xB8, 0x12, 0x6F, 0x28},
                      {0xCD, 0x8A, 0x70, 0x56, 0x72, 0xF9, 0xBF, 0x4F, 0x73, 0xE9, 0xF7, 0x57,
0x16, 0xAC, 0x50, 0xC0},
                      {0x9D, 0xB7, 0x47, 0x71, 0x60, 0xC4, 0x74, 0x43, 0x6C, 0x1F, 0x93, 0x77,
0xDC, 0xCE, 0x20, 0x8C},
                      {0x99, 0x5F, 0x44, 0x01, 0xF5, 0x1E, 0x87, 0x5E, 0x61, 0x2C, 0x4B, 0x1D,
0x81, 0x15, 0xF4, 0x23},
                      {0xD6, 0xEA, 0xE1, 0x67, 0xF1, 0x7F, 0xFE, 0xDA, 0x3C, 0x07, 0x53, 0x6A,
0x84, 0x9C, 0xCB, 0x02},
                      {0x83, 0x33, 0xDD, 0x35, 0xE2, 0x59, 0x5A, 0x98, 0xA5, 0x92, 0x64, 0x04,
0x06, 0x10, 0x4D, 0x1C},
                      {0x97, 0x08, 0x31, 0xEE, 0xAB, 0x05, 0xAF, 0x79, 0xA0, 0x18, 0x46, 0x6D,
0xFC, 0x89, 0xD4, 0xC7},
                      {0xFF, 0xF0, 0xCF, 0x42, 0x91, 0xF8, 0x68, 0x0A, 0x65, 0x8E, 0xB6, 0xFD,
0xC3, 0xEF, 0x78, 0x4C},
```

```
                    {0xCC, 0x9E, 0x30, 0x2E, 0xBC, 0x0B, 0x54, 0x1A, 0xA6, 0xBB, 0x26, 0x80,
0x48, 0x94, 0x32, 0x7D},
                    {0xA7, 0x3F, 0xAE, 0x22, 0x3D, 0x66, 0xAA, 0xF6, 0x00, 0x5D, 0xBD, 0x4A,
0xE0, 0x3B, 0xB4, 0x17},
                    {0x8B, 0x9F, 0x76, 0xB0, 0x24, 0x9A, 0x25, 0x63, 0xDB, 0xEB, 0x7A, 0x3E,
0x5C, 0xB3, 0xB1, 0x29},
                    {0xF2, 0xCA, 0x58, 0x6E, 0xD8, 0xA8, 0x2F, 0x75, 0xDF, 0x14, 0xFB, 0x13,
0x49, 0x88, 0xB2, 0xEC},
                    {0xE4, 0x34, 0x2D, 0x96, 0xC6, 0x3A, 0xED, 0x95, 0x0E, 0xE5, 0x85, 0x6B,
0x40, 0x21, 0x9B, 0x09},
                    {0x19, 0x2B, 0x52, 0xDE, 0x45, 0xA3, 0xFA, 0x51, 0xC2, 0xB5, 0xD1, 0x90,
0xB9, 0xF3, 0x37, 0xC1},
                    {0x0D, 0xBA, 0x41, 0x11, 0x38, 0x7B, 0xBE, 0xD0, 0xD5, 0x69, 0x36, 0xC8,
0x62, 0x1B, 0x82, 0x8F}};


    static Set<String> subMix = new HashSet<>();
    static List<int[][]> arrays = new ArrayList<>();
    static StringBuilder stringBuilder;
    static StringBuilder stringBuilderLmax;

    static double XnMax = 3/Math.pow(2,4);
    static double XlMax = 9/Math.pow(2,8);

    public static double [][][] M ;

    static int FxNmax = 0;
    static int FxLmax = 0;

    public static int [][] resTable = new int[256][256];
    public static void main(String[] args) {

        stringBuilder = new StringBuilder();
        stringBuilderLmax = new StringBuilder();
        double e = 0;
        while (subMix.size() < 2000) {
            int[][] tmp = sBox.clone();
            Util.shuffle(tmp);
            String tmpString = Arrays.deepToString(tmp);

            if (subMix.add(tmpString)) {
                M = new double[4][256][256];
                for (int i = 0; i <= 255; i++) {
                    for (int j = 0; j <= 255; j++) {
                        resTable[i][j] = Util.vectorMultiplication2(i, j);
                    }
                }

                for (int alpha = 0; alpha <= 255; alpha++) {

                    for (int u = 0; u <= 1; u++) {

                        for (int z = 0; z <= 255; z++) {

                            for (int x = 0; x <= 255; x++) {
                                int I = x + Util.submission(tmp, z) + u;
                                int pow1 = resTable[Util.summ8(Util.summ8(x,
Util.submission(tmp, z)), u)][alpha];
                                int pow2 = resTable[x][alpha];
                                if (Util.MSB(I) == 0) {
```

```
                                    M[2 * u][alpha][z] = M[2 * u][alpha][z] + Math.pow(-1,
Util.summ2(pow1, pow2));
                                } else {
                                    M[2 * u + 1][alpha][z] = M[2 * u + 1][alpha][z] +
Math.pow(-1, Util.summ2(pow1, pow2));
                                }
                            }
                        }
                    }
                }
        for (int i = 0; i <= 255; i++) {
            for (int j = 0; j <= 255; j++) {
                System.out.print(M[0][i][j] + " ");
            }
            System.out.println();
        }

                for (int j = 0; j <= 3; j++) {
                    for (int i = 0; i <= 255; i++) {
                        Util.Hadamar(M[j][i], 8);
                    }
                }


        BufferedWriter writer = null;
        for (int k = 0; k <=3; k++) {
            File logFile = new File("matrix"+Integer.toBinaryString(k));
            try {
                writer = new BufferedWriter(new FileWriter(logFile));
            for (int i = 0; i <= 255; i++) {
                for (int j = 0; j <= 255; j++) {
                    writer.write(M[k][i][j] + " ");
                }
                writer.newLine();
            }
            } catch (IOException e) {
                e.printStackTrace();
            } finally {
                try {
                    writer.close();
                } catch (IOException e) {
                    e.printStackTrace();
                }
            }
        }


                M[0][0][0] = 0;
                M[1][0][0] = 0;
                M[2][0][0] = 0;
                M[3][0][0] = 0;

                int max = 0;
                int alpha = 0;
                int beta = 0;
                for (int i = 0; i < 256; i++) {
                    for (int j = 0; j < 256; j++) {
                        int res1 = Math.abs((int) M[0][i][j]) + Math.abs((int) M[1][i][j]);
                        int res2 = Math.abs((int) M[2][i][j]) + Math.abs((int) M[3][i][j]);
                        int res = Util.getBigger(res1, res2);
```

```
                        if (res > max) {
                            max = res;
                            alpha = i;
                            beta = j;
                        }

                    }
                }

                double Lmax = 0;

                for (int a = 1; a <= 255; a++) {
                    for (int b = 1; b <= 255; b++) {
                        double tmpL = 0;
                        for (int u = 0; u <= 255; u++) {
                            tmpL+=Math.pow(-1, (resTable[u][a] +
resTable[Util.submission(tmp, u)][b])%2);
                        }

                        tmpL = Math.pow(tmpL/Math.pow(2, 8), 2);
                        if (tmpL > Lmax) {
                            Lmax = tmpL;
                            System.out.println("Lmax " + Lmax);
                        }
                    }
                }
                double nMaxTmp = max / Math.pow(2, 16);
                if (nMaxTmp < XnMax)  FxNmax++;
                if (Lmax < XlMax)  FxLmax++;
                System.out.println(nMaxTmp + " ========= " + Lmax+" "+ e/10 + " %");
                e++;
               // stringBuilder.append(nMaxTmp).append("\r\n");
               // stringBuilderLmax.append(Lmax ).append("\r\n");

            }

        }

       /* File logFile = new File("ResNmax.txt");
        File logFileL = new File("ResLmax.txt");
        BufferedWriter  writer = null;
        BufferedWriter  writerL = null;
        try {

            writer = new BufferedWriter(new FileWriter(logFile));
            writerL = new BufferedWriter(new FileWriter(logFileL));
            writerL.write(stringBuilderLmax.toString());
            writer.write(stringBuilder.toString());
        } catch (IOException g) {
            g.printStackTrace();
        } finally {
            try {
                writer.close();
                writerL.close();
            } catch (IOException g) {
                g.printStackTrace();
            }
        }*/
```

```
        System.out.println("FxNmax " + FxNmax);
        System.out.println("FxLmax " + FxLmax);
    }
}
```

Додаток Б

Програмний код реалізації методу обґрунтування стійкості SNOW 2.0-подібних шифрів відносно кореляційних атак

Програмна реалізація виконана на ПК з процесором Intel(R) Core(TM) i7, 2.2 GHz та обсягом оперативної пам'яті 16 ГБ на базі ОС macOS Mojave 10.14. Мова програмування – Java. Середовище розробки Intelij Idea.

```
// Файл SecurityBinary.java

public class SecurityBinary {
        public static void main(String[] args) {
            int n = 16;
            int p = 8;
            int t = 8;
            int k = 4;

            double lMax = 9.0 / Math.pow(2, 8);

            int l = n * p;

            double deltaC = 0.000073;

            double deltaK = (Math.pow(2, t) - 1) * Math.pow(lMax, 20);

            int eta = 3;
            System.out.println(" " + deltaK);
            double[] tLArray = new double[n * p - 1];

            for (int i = 1; i <= tLArray.length; i++) {
                double mk = 2 * i * t * 0.69314718056 / deltaK;
                double tL = Math.pow(mk, 1 / eta) * k * Math.pow(2, t * (l - i) / eta) + t *
(mk + t * i * Math.pow(2, t * i)) + Math.pow(2, t * (i + 1));
                tLArray[i - 1] = tL;
            }


            int lmin = 0;
            double min = Double.MAX_VALUE;
            for (int i = 0; i < tLArray.length; i++) {
                if (tLArray[i] < min) {
                    min = tLArray[i];
                    lmin = i + 1;
                }
            }

            System.out.printf(" %f", min);
            System.out.println(Utils.log(min, 2));

            double tmp = k * Math.pow(2, t * (l - lmin) / eta) * Math.pow(2 * lmin * t *
0.69314718056, 1 / eta) * Math.pow(deltaK, -1 / eta);
```

```
            System.out.println(Util.log(min, 2));
            double NL = 4 * Math.pow(2, t * (l - lmin) / eta) * Math.pow(2 * lmin * t *
0.69314718056, 1 / eta) * Math.pow(deltaK, -1 / eta);
            System.out.println("NL " + Util.log(NL, 2));
        }

// Файл SecurityModular.java

public class SecurityModular {
        public static void main(String[] args) {
            int n = 16;
            int p = 8;
            int t = 8;
            int k = 4;

            double nMax = 3/Math.pow(2,4);

            int l = n * p;

            double deltaC = 0.000073;

            double deltaK = (Math.pow(2, t) - 1) * Math.pow(nMax, 40);

            int eta = 3;
            System.out.println(" " + deltaK);
            double[] tNArray = new double[n * p - 1];

            for (int i = 1; i <= tNArray.length; i++) {
                double mk = 2 * i * t * 0.69314718056 / deltaK;
                double tN = Math.pow(mk, 1 / eta) * k * Math.pow(2, t * (l - i) / eta) + t *
(mk + t * i * Math.pow(2, t * i)) + Math.pow(2, t * (i + 1));
                tLArray[i - 1] = tL;
            }


            int nmin = 0;
            double min = Double.MAX_VALUE;
            for (int i = 0; i < tNArray.length; i++) {
                if (tNArray[i] < min) {
                    min = tNArray[i];
                    nmin = i + 1;
                }
            }

            System.out.printf(" %f", min);
            System.out.println(Utils.log(min, 2));

            double tmp = k * Math.pow(2, t * (l - nmin) / eta) * Math.pow(2 * nmin * t *
0.69314718056, 1 / eta) * Math.pow(deltaK, -1 / eta);
            System.out.println(Util.log(min, 2));
            double Nn = 4 * Math.pow(2, t * (l - nmin) / eta) * Math.pow(2 * lmin * t *
0.69314718056, 1 / eta) * Math.pow(deltaK, -1 / eta);
            System.out.println("Nn " + Util.log(Nn, 2));
        }


// Файл Util.java


import java.util.Random;
```

```
public class Util {
    public static int MSB(int n) {
        return (n & 0xff) >> 7;
    }

    public static int submission(int [][] sBox, int array){
        int row = array/16;
        int col = array%16;
        return sBox[row][col];
    }

    public static int summ8(int a, int b){
        return (a+b)%256;
    }

    public static int summ2(int a, int b){
        return (a+b)%2;
    }

    public static int vectorMultiply(int [] a, int [] b){
        int summ = 0;
        for (int i = 0; i < a.length; i++){
            summ+=a[i]*b[i];
        }

        return summ;
    }

    public static void Hadamar( double[] d, int t)
    {
        double[] c = new double[d.length];

        for (int j = t; j > 0; j--)
        {
            int k = 1 << (j - 1);
            for (int i = 0; i < d.length; i++)
            {
                if (i % (2 * k) < k)
                {
                    c[i] = d[i] + d[i + k];
                }
                else
                {
                    c[i] = d[i - k] - d[i];
                }
            }

            for (int i = 0; i < d.length; i++)
            {
                d[i] = c[i];
            }
        }
    }


    public static int[] convertBinary(int decimalNumber) {
        //initialize array
        int binary[] = new int[8];
        int index = 0;
```

```
        //loop till the number is greater than 0
        while (decimalNumber > 0) {
            //divide the number by 2 using modulus operator so that we get the remainder
            int remainder = decimalNumber % 2;
            //store the remainder in array
            binary[index++] = remainder;
            //divide the number to get the quotient and assign it back to the number
            decimalNumber = decimalNumber / 2;
        }
        return binary;
    }

    public static int vectorMultiplication2(int a, int b){
        int [] aV = convertBinary(a);
        int [] bV = convertBinary(b);
        int summ = 0;
        for (int i = 0; i <=7; i++){
            summ+=aV[i]*bV[i];
        }
        return summ%2;
    }

    public static double matrixDeterminant (double[][] matrix) {
        double temporary[][];
        double result = 0;

        if (matrix.length == 1) {
            result = matrix[0][0];
            return (result);
        }

        if (matrix.length == 2) {
            result = ((matrix[0][0] * matrix[1][1]) - (matrix[0][1] * matrix[1][0]));
            return (result);
        }

        for (int i = 0; i < matrix[0].length; i++) {
            temporary = new double[matrix.length - 1][matrix[0].length - 1];

            for (int j = 1; j < matrix.length; j++) {
                for (int k = 0; k < matrix[0].length; k++) {
                    if (k < i) {
                        temporary[j - 1][k] = matrix[j][k];
                    } else if (k > i) {
                        temporary[j - 1][k - 1] = matrix[j][k];
                    }
                }
            }

            result += matrix[0][i] * Math.pow (-1, (double) i) * matrixDeterminant
(temporary);
            System.out.println(result);
        }
        return (result);
    }

    public static double[] getMax(double [][] M){
        double max = 0;
        double alpha = 0;
        double beta = 0;
```

```
    double [] res = new double[3];
    for (int i = 0; i < 256; i++){
        for (int j =0; j < 256; j++){
            int abs = Math.abs((int)M[i][j]);
            if (abs > max){
                max = abs;
                alpha = i;
                beta = j;
            }
        }
    }

    res[0] = max;
    res[1] = alpha;
    res[2] = beta;

    return res;
}

public static int getBigger(int a, int b){
    return a>b?a:b;
}
public static double log(double x, int base)
{
    return  (Math.log(x) / Math.log(base));
}

public  static  void  shuffle(int[][] a) {
    Random random = new Random();

    for (int i = a.length - 1; i > 0; i--) {
        for (int j = a[i].length - 1; j > 0; j--) {
            int m = random.nextInt(i + 1);
            int n = random.nextInt(j + 1);

            int temp = a[i][j];
            a[i][j] = a[m][n];
            a[m][n] = temp;
        }
    }
}
```

Прим. № 1

"ЗАТВЕРДЖУЮ"
Заступник директора департаменту –
начальник управління
Служби зовнішньої розвідки України

Романович К.О.

"13" 02 2019 року

АКТ
впровадження результатів дисертаційної роботи Поремського Михайла Васильовича в науково-дослідній роботі «Розроблення та адаптація математичних методів аналізу систем криптографічного захисту інформації з урахуванням сучасних вимог інформаційного середовища» (шифр «Корифена»)

Комісія у складі голови комісії Седікіна С.К. та членів комісії: Черевка Ю.П., Гришакова С.В. з'ясувала, що в Службі зовнішньої розвідки України в результаті виконання науково-дослідної роботи «Дослідження, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем» (шифр «Аргус») вперше впроваджено отриманий Поремським Михайлом Васильовичем **такий науковий результат:**

Нижня межа інформаційної складності кореляційних атак на потокові шифри, яка містить явну залежність від ймовірності помилки атаки.

Ефект від впровадження зазначеного наукового результату полягає в тому, що він дозволяє встановлювати найменшу кількість рівнянь у системі зі спотвореними правими частинами (незалежно від способу її побудови або методу розв'язання), за якої ймовірність помилкового відновлення її істинного розв'язку не перевищує задану величину. Це має важливе значення для побудови оцінок стійкості SNOW 2.0-подібних потокових шифрів відносно сучасних кореляційних атак над скінченними полями характеристики 2.

Голова комісії: _____ Седінкін С.К.

Члени комісії:
к.т.н. _____ Черевко Ю.П.

к.т.н. _____ Гришаков С.В.

"12" 02 2019 року

Прим. № 1

"ЗАТВЕРДЖУЮ"
Заступник директора департаменту –
начальник управління
Служби зовнішньої розвідки України

Романович К.О.

"13" 02 2019 року

АКТ

впровадження результатів дисертаційної роботи Поремського Михайла Васильовича в науково-дослідній роботі «Розроблення та адаптація математичних методів аналізу систем криптографічного захисту інформації з урахуванням сучасних вимог інформаційного середовища» (шифр «Корифена»)

Комісія у складі голови комісії Седікіна С.К. та членів комісії: Черевка Ю.П., Гришакова С.В. з'ясувала, що в Службі зовнішньої розвідки України в результаті виконання науково-дослідної роботи «Розроблення та адаптація математичних методів аналізу систем криптографічного захисту інформації з урахуванням сучасних вимог інформаційного середовища» (шифр «Корифена») вперше впроваджено отримані Поремським Михайлом Васильовичем **такі наукові результати:**

1. Аналітичний вираз параметра, що визначає стійкість SNOW 2.0-подібних шифрів відносно відомих кореляційних атак в термінах коефіцієнтів Фур'є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки.
2. Метод обґрунтування стійкості SNOW 2.0-подібних потокових шифрів (ПШ) відносно відомих кореляційних атак безпосередньо за параметрами компонент алгоритмів потокового шифрування.

Ефект від впровадження зазначених наукових результатів полягає в тому, що вони дозволяють:

– ввести науково обґрунтовані параметри вузлів заміни SNOW 2.0-подібних ПШ, що характеризують їх стійкість відносно відомих кореляційних атак;
– скоротити (*не менш як у 32 рази*) час обчислення зазначених параметрів завдяки застосуванню розробленого дисертантом алгоритму;
– встановити існування двійкової кореляційної атаки на SNOW 2.0, яка є більш ніж у 2^{40} разів швидше в порівнянні з найкращою раніше відомою двійковою атакою;
– підвищити обґрунтованість експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Голова комісії: Седінкін С.К.

Члени комісії:
к.т.н. Черевко Ю.П.

к.т.н. Гришаков С.В.

"12" 02 2019 року

„ЗАТВЕРДЖУЮ”
Виконавчий директор АТ „ІІТ”
_____В.Д.Кравченко
“26” 09 2019 р.

АКТ
впровадження результатів досліджень дисертаційної роботи
Поремського Михайла Васильовича в акціонерному товаристві
„Інститут Інформаційних Технологій” м. Харків

Комісія у складі голови комісії головного конструктора професора Горбенка Івана Дмитровича та членів комісії заступників головного конструктора професора Потія Олександра Володимировича та професора Качко Олени Григорівни з’ясувала, що в АТ "ІІТ" вперше впроваджено отримані Поремським Михайлом Васильовичем наукові результати, що на даний момент використані в Інституті Інформаційних Технологій під час розроблення та прийняття національного стандарту ДСТУ 8845-2019, шифр « Струмок».

1. Метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2.
2. Метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2.

Ефект від впровадження зазначених наукових результатів полягає в тому, що вони дозволяють:

– ввести науково обґрунтовані параметри вузлів заміни (двійкових та модулярних) SNOW 2.0-подібних шифрів, що характеризують їх стійкість відносно відомих кореляційних атак;

– скоротити (принаймні, у 2^{11} разів) час обчислення зазначених параметрів завдяки застосуванню розробленого дисертантом алгоритму;

– обґрунтувати практичну стійкість національного стандарту потокового шифрування України “Струмок” відносно відомих кореляційних атак (на рівні 2^{249} операцій за наявності не менше ніж 2^{249} знаків гами);

– підвищити обґрунтованість експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Голова комісії І.Д. Горбенко

Члени комісії:

О.В. Потій

О.Г.Качко